Research and Background

For Patient Consent Policy Recommendation

White Paper

Created by the Patient Consent and Informing Task Group

Of the Privacy Steering Team

December 7, 2011

This document does not reflect the final recommendations or approval of the content by CalOHII or its Steering Teams, nor the policy, approval, or adoption of the content by the California Health and Human Services Agency (CHHS), unless otherwise specifically indicated in the document. The documents are utilized for discussion and development for future recommendations to CalOHII.

Table of Contents

Version	Name	Date	Description
1.0		12/7/2011	Initial version of paper

Executive Summary

This is a first in a series of white papers documenting the collaborative efforts under the guidance of the California Office of Health Information and Integrity (CalOHII) to recognize and support the goal of national health reform by proactively developing the foundational framework in which an effective electronic exchange of health information in California could progress. Since 2001, California has recognized, supported, and has been working on developing policies and guidance for electronic health information exchanges (HIE).

The National Coordinator for Health Information Technology wrote in an article published in Health Affairs in June 2010 that the HITECH Act's provisions for health information exchange and technology laid the cornerstone and infrastructure for national health reform. Not coincidentally, the HITECH Act proclaims a strategic goal to ensure that each person in the United States has an electronic health record by 2014, which is when many of the Affordable Care Act's provisions are scheduled to take effect, after the adoption and meaningful use of electronic medical records currently underway.

As awarded in spring of 2010, a four-year cooperative agreement between CHHS and ONC, California Office of Health Information Integrity (CalOHII) will utilize $38.8 million in ARRA funds to support electronic HIEs across the state of California.

Assembly Bill 278 (Stat. 2010 Ch. 227 (Monning), codified at Health and Safety Code § 130275 et seq.), authorizes the Director of CalOHII to approve demonstration projects for electronic exchange of health information. CalOHII has the general authority to enforce State laws mandating the confidentiality of medical information. These projects will test policies and rules to better inform the State and health care stakeholders while the infrastructure for the electronic exchange of health information is being defined over the next several years. By allowing for various demonstration projects, it will be possible to determine how best to protect privacy in accordance with State and Federal laws while enabling electronic exchange of health information.

The CalPSAB Principles of Fair Information Practices were developed in 2009 and have been adopted and included in the regulations of the demonstration projects for the electronic exchange of health information. The Principles are being required to establish the foundation for trust in the exchange of an individuals' health information. Patients must trust that the health information exchange system will securely share their information when appropriate; providers must trust that the information exchanged is

relevant, accurate, and current; Health information organizations (HIO) must trust their partners in exchanging health information.

Demonstration projects will allow California to test privacy and security policy that will increase the trust of HIE participants by elevating protection of health information through innovative technology and sound business practice. Currently, there are two demonstration projects approved by CalOHII in California, and CalOHII looks forward to working with these two innovative and progressive organizations as we test privacy and security policies for electronic exchange of health information. It is necessary for health systems to work together in order to compile the complete experience of a patient's care and ensure accessibility of that information to clinicians as the patient moves through various health care settings. The Demonstration Project Participants will support clinicians in making cost-effective, fact-based decisions that will reduce medical errors, decrease redundant tests, and improve care coordination with the timely access to their patients' data.

One of the most important elements in creating an interoperable electronic exchange of health information for the demonstration projects is patient consent. It is important to emphasize that consent policies must be accompanied by privacy and security protections relating to authentication, authorization, access controls and auditing to earn patient trust. The consent must also satisfy all federal and California laws and regulations. In order for consent to be meaningful, an individual must be informed of certain information on which to make an educated decision. The notion of meaningful consent is foundational in most iteration of Fair Information Practice Principles. Both the CalPSAB principles as well as the Federal Privacy and Security Tiger Team recommendations recognize the need for meaningful consent.

The research and recommendations included in this document are a starting point for the comprehensive privacy and security policies that will be recommended by CalOHII for the demonstration projects. Results from the demonstration projects will inform the California legislature of the outcomes, best practices, and the need for harmonization with federal privacy and security law.

Introduction

This document sets forth research and recommendations surrounding the collection, use, access and disclosure of health records in an electronic exchange of health information. The information collected in this document was compiled by steering teams and task groups of stakeholder representatives convened by CalOHII.

This document does not reflect the final recommendations or approval of the content by CalOHII or its Steering Teams, nor the policy, approval, or adoption of the content by the California Health and Human Services Agency (CHHS), unless otherwise specifically indicated in the document. The documents are utilized for discussion and development for future recommendations to CalOHII.

This document will provide the historical background and research undertaken that has led to the current opt-in consent policy recommendation. The six areas of focus are:

1. The Federal landscape
2. The California landscape with respect to the existing electronic health information exchange infrastructure
3. The CalOHII background and structure
4. The demonstration projects for the electronic exchange of health information
5. Overview of consent models
6. The opt-in consent policy
7. The education component of the patient consent process

Federal Landscape

Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act in February 2009, as part of the federal stimulus bill, the American Recovery and Reinvestment Act. Congress subsequently enacted the Patient Protection and Affordable Care Act (PPACA) in March 2010, with landmark provisions for health reform. As the National Coordinator for Health Information Technology wrote in an article published in Health Affairs in June 2010, the HITECH Act's provisions for health information exchange and technology laid the cornerstone and infrastructure for national health reform. Not coincidentally, the HITECH Act proclaims a strategic goal to ensure that each person in the United States has an electronic health record by 2014, which is when many of the Affordable Care Act's provisions are scheduled to take effect, after the adoption and meaningful use of electronic medical records currently underway.

The HITECH Act's provisions have defined and driven the compressed efforts and deadlines in California. The stakeholder process to generate California's strategic and operational plans for health information exchange occurred in the second half of 2009 and first quarter of 2010. In February 2010, the United States Department of Health and Human Services (DHHS) awarded California a $38.5 million grant to support the expansion of health information exchange in California. In 2010 the California Health and Human Services Agency (CHHS) designated Cal eConnect as the governance

entity to administer the grant over the next three years. California submitted its strategic and operational plans to ONC on April 2010.

ONC/Tiger Team

As stated in the Consumers Union and Center for Democracy and Technology briefing paper to CHHS dated October 6, 2010, "The 2010 Health IT Policy Committee was created by law to make recommendations to the National Coordinator for Health IT on a policy framework to promote nationwide HIE. The Policy Committee is chaired by the National Coordinator. The Privacy and Security "Tiger Team" was formed as part of the Policy Committee to develop effective privacy and security policies for electronic HIE. In August 2010, the Tiger Team released a set of recommendations for entities participating in the first stage of the federal "meaningful use" incentives program. Later that month, the Policy Committee adopted the Tiger Team's recommendations without modification. The U.S. Department of Health and Human Services is now considering how to implement them."

Tiger Team Recommendation

In the same letter Consumers Union and Center for Democracy and Technology states: "The Tiger Team's approach requires meaningful patient consent where information exchanges would place patient data outside the provider's control, but does not require patient consent for directed exchange. Instead, the Tiger Team's approach protects the privacy and security of both types of exchanges with the full spectrum of fair information practices. This framework is compliant with both the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the California Medical Information Act (CMIA).

HIPAA and CMIA permit providers to disclose patient information for treatment purposes without patient consent. Under the law, providers can do this by paper mail, fax, and electronic exchange. In directed electronic exchange between providers, just as in the paper world, the provider remains largely in control of decisions about disclosures from a patient's record (for example, what information should be sent and to whom). This model of transaction is the foundation upon which HIPAA and CMIA are built. In both laws, consent is generally not required for providers to share information for treatment and treatment-related purposes. Such directed exchange of health information is part of the traditional model of treatment, like forwarding a patient's paper records to another doctor for consultation."

In California, CalPSAB took the Tiger Team recommendation into consideration and invited the chair of the Tiger Team to present its recommendation to CalPSAB in December of 2010. In conclusion, CalPSAB adopted an opt-in patient consent recommendation based on patient California constitutional right to privacy and conveyed its recommendation to the CHHS Secretary via a letter in January 2011 (Appendix C: CalPSAB Letter to Secretary Dooley).

California Landscape

As the authoritative state agency for the governance of health related programs, such as health care services and social services and related provisions, CHHS oversees the many activities carried out by various state departments and offices under its authority. Under Governor's Executive Order S-06-07 CHHS was tasked, in cooperation with the State Chief Information Officer, the Business, Transportation and Housing Authority, and key public and private stakeholders, to accelerate the use of health information technology and provide support for uniform interoperability standards and adoption of health information technologies.

California Office of Health Information Integrity

Background and Organizational Structure

Following its establishment in 2001 as the California Office of HIPAA Implementation (CalOHI), the Office changed its name to the Office of Health Information Integrity (CalOHII) in August 2008. This change was made to reflect CalOHII's expanding new role supporting the Health and Human Services Agency's health information exchange initiatives.

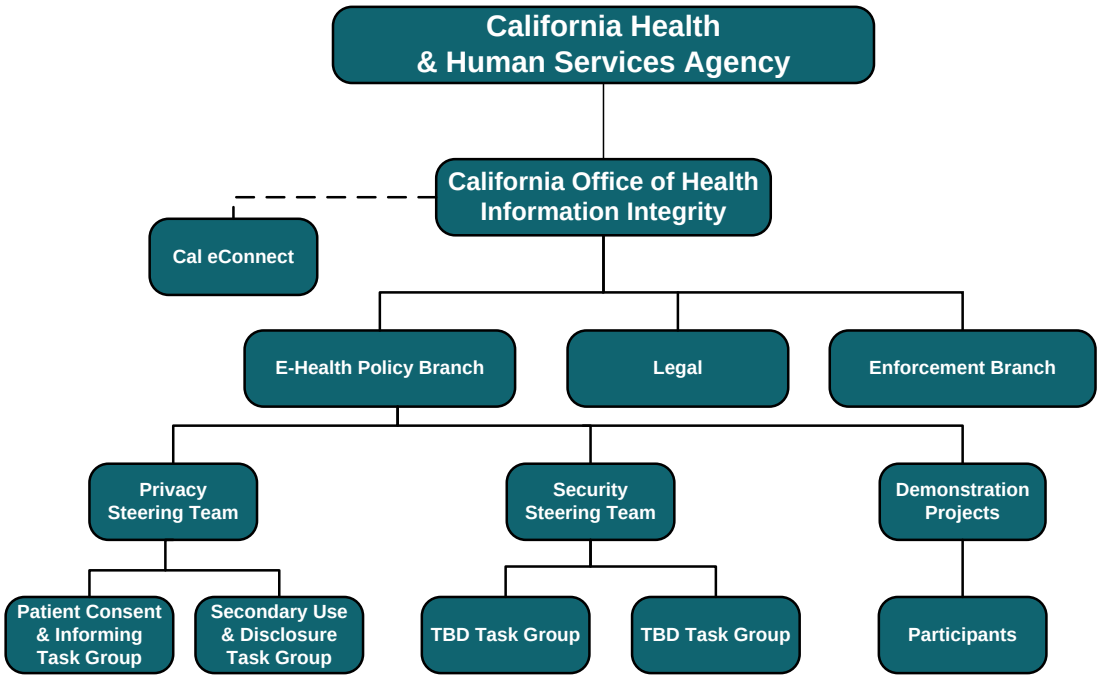
CalOHII also serves as the primary resource for state entities on health information privacy and the implementation of HIPAA regulations. CalOHII will continue to fulfill its statutory role to provide technical assistance and ensure uniform and cost effective HIPAA implementation. CalOHII also has the general authority to enforce State laws mandating the confidentiality of medical information.

In October 2007, then-Secretary Kim Belshé announced the formation of a new Privacy and Security Advisory Board (CalPSAB) composed of various stakeholder representations to develop and recommend new policies and standards related to privacy and security of health information. CalOHII served, from 2007 till 2011, as the organization supporting and facilitating CalPSAB and the policies and standards

development process. Following the elimination of CalPSAB in the May Revise Budget of 2011, the close collaboration between CalOHII and the wide spectrum of stakeholders continues through the work and efforts of the Privacy Steering Team, the Security Steering Team, and the task groups formed by these steering teams. The steering teams and task groups recommend privacy and security policies for the electronic exchange of health information, as well as contribute to the harmonization of California and federal privacy and security law. Beginning in the second half of 2011, the Privacy Steering Team began focusing on law harmonization efforts.

The following chart represents the current CalOHII organizational structure.

California HIE Privacy and Security Structure



For additional information regarding CalOHII, please visit the website at: www.ohi.ca.gov.

CalPSAB Achievements

The two main achievements of CalPSAB were the approval of the Principles of Fair Information Practices and the recommendation of an affirmative opt-in patient consent

policy. Additionally, CalPSAB also approved, through a survey process, a set of security guidelines in 2010.

Principles of Fair Information Practices

As part of its achievements, CalPSAB gained the approval of the Secretary, California Health and Human Services Agency, of a set of principles for fair information practices. These Principles (Table 1: CalPSAB Principles of Fair Information Practices) have been adopted and included in the regulations of the demonstration projects for the electronic exchange of health information, and are reflected below.

Table 1: CalPSAB Principles of Fair Information Practices

PRINCIPLES
1. **Openness** – There should be a general policy of openness among entities that participate in electronic health information exchange about developments, practices, and policies with respect to individual health information.
2. **Individual Health Information Quality** –Health information shall be relevant, accurate, complete, and kept up-to-date**.**
3. Individual Participation – Individuals have the right to: a. Ascertain the person responsible for individual health information for an entity, obtain confirmation of whether the entity has specific individual health information relating to the individual, and obtain its location. b. Receive their individual health information in a reasonable time and manner, at a reasonable charge, and in a format that is generally accessible by individuals. c. Challenge the accuracy of their individual health information and, if successful, to have the individual health information corrected, completed, or amended. d. Control the access, use, or disclosure of their individual health information, unless otherwise specified by law or regulation.
4. **Collection Limitation –** There shall be limits to the collection of individual health information. Individual health information shall be obtained by lawful and fair means. Where appropriate, it shall be obtained with the knowledge or consent of the individual. The specific purposes for which individual health information is collected shall be specified not later than at the time of collection.
5. **Individual Health Information Limitation** – Use and disclosure of individual health information shall be limited to the specified purpose. Certain use and disclosure shall require consent.

PRINCIPLES

6. **Purpose Limitation -** Individual health information shall be relevant to the purpose for which it is to be used and, limited to the minimum information necessary for the specified purpose. The subsequent use shall be limited to the specified purpose.

7. **De-Identified Information –**De-identified individual health information shall not be re-identified unless specified in law. If de-identified individual health information is re-identified, it shall be subject to these principles. De-identified individual health information shall not be disclosed if there is a reasonable basis to believe that the information can be used to identify an individual.

8. **Security Safeguards –** Individual health information should be protected by appropriate security safeguards against such risks as loss or destruction, unauthorized access, use, modification or disclosure of data.

9. **Accountability –** An entity shall comply with laws, regulations, standards and organizational policies for the protection, retention and destruction of individual health information. Any person who has access to individual health information shall comply with those provisions.

The Principles are being required to establish the foundation for trust in the exchange of an individuals' health information. Patients must trust that the health information exchange system will securely share their information when appropriate; providers must trust that the information exchanged is relevant, accurate, and current; HIOs must trust their partners in exchanging health information.

The intention is for the incorporation of these principles into an entity's business practices at a high level to create the foundation for trust amongst all parties. Where specific laws direct a certain course of action, the more specific requirements would apply. For instance, Principle 3(c) requires a procedure for an individual to challenge the accuracy of their health information, but does not specify the method. HIPAA permits individuals to request that their medical record be amended (45 CFR 164.526), while the California Patient Access to Health Records Act (Health and Safety Code section 123111) permits an addendum. In this example, Federal and State law would specify the procedure provided by the principle.

These Principles, specific to California, were developed over a two year period through the CalPSAB stakeholder process and unanimously agreed upon. The principles then were posted on the CalOHII website for 30 days and were emailed to the over 400 interested parties on the CalPSAB contact list for public comment. Subsequently, the

Secretary of the Health and Human Services Agency approved the principles and they were posted on CalOHII's website as 9 recommended principles for electronic health information exchange in California.

The Principles are based upon a variety of successful principles for privacy and security of individual information, including Connecting for Health – Markle (9 Principles), Consumer Union Guiding Principles, Health Privacy Working Group (11 Principles), E-Health Initiative connecting Communities Common Principles, Organization for Economic Co-Operation and Development Fair Information Practice (8 Principles), Japan Personal Information Protection Act (5 Principles), Asia Pacific Economic Cooperation (9 Principles), and the European Union (9 principles).

The Data Protection Directive (http://en.wikipedia.org/wiki/Data_Protection_Directive) is a European Union directive which regulates the processing of personal data within the European Union. It is an important component of EU privacy and human rights law. In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data." The seven principles governing the OECD's recommendations for protection of personal data were: Notice, Purpose, Consent, Security, Disclosure, Access, and Accountability.

It is expected that as a result of adopting these Principles, there would be improved health care outcomes, reduced costs, and improved public and population health. To this end, CHHS' California eHealth Initiative has set forth the following seven goals:

1. To ensure patients have safe, secure access to their personal health information and the ability to share that information with others involved in their care
2. To engage in an open, inclusive, collaborative, public-private process that supports widespread EHR adoption and a robust, sustainable statewide health information exchange
3. To improve health care outcomes and reduce costs
4. To maximize California stakeholders' collective access to critical ARRA stimulus funds
5. To integrate and synchronize the planning and implementation of HIE, HIT, telehealth and provider incentive program components of the federal stimulus act
6. To ensure accountability in the expenditure of funds
7. To improve public and population health through stronger public health program integration, bio-surveillance and emergency response capabilities

Opt-In Patient Consent Policy

After the adoption of the principles, CalPSAB began the development of a consent policy. In 2008, following a symposium that bore no clear outcome, CalPSAB grappled with the issue, examining the legal concerns, policy issues, the implementation issues, and need for patient education.

CalPSAB discussed that outside of a narrow set of circumstances, a "no consent" policy would present potential liability that would be unjustified. Considering the lack of transparency for the use and disclosures of health information in the current health system, combined with California's explicit Right to Privacy, the stakeholder community decided against a "no consent" policy for the exchange of health information.

In late 2009, CalPSAB adopted a bifurcated system of consent. This system had an "opt-out" model for general HIE but an "opt-in" model for any sensitive health information. Upon receiving nearly unanimously negative comments regarding the bifurcated system, from the involved stakeholders and hundreds of individuals, the proposal was withdrawn. The CalPSAB continued to discuss the matter, considered the risks and implementation issues, including the lack of ability to segregate sensitive health information, and in October of 2010 adopted an "opt-in" consent policy which was confirmed in a letter to Secretary Dooley in January 2011 (Appendix C: CalPSAB Letter to Secretary Dooley). Given the lengthy deliberation process of the CalPSAB, along with independent legal analysis, CalOHII has adopted the general stance of the CalPSAB. This decision is reflected in the affirmative consent requirement in the demonstration project regulations. The regulations make a slight differentiation between direct exchange and exchange through an HIO, based on stakeholder feedback and the potential operational challenges presented by affirmative consent.

The demonstration project regulations include special provisions for Participants to request to "Demonstrate Alternative Requirements" (DAR process). These provisions allow Participants to test other requirements and policies that may differ from the provisions outlined in the regulations. The DAR process will examine the unique circumstances of the Participant and allow for alternative policy options to be tested. For example, although the regulations require an Opt-In Consent policy, a Participant utilizing an Opt-Out Consent policy for their organization may request a DAR if they meet the specific requirements outlined in the regulations. The DAR process is intended to allow California to test other models of policy that may not be included in the current set of regulations or are different, but commensurate.

American Recovery and Reinvestment Act and Cal eConnect

California Budget Bill of 2010, Senate Bill 853 (Chapter 717), added California Health Information Technology Act codified in Health and Safety Code Section 130250.1. This Act allows CHHS to apply for federal funds made available through American Recovery and Reinvestment Act of 2009 (ARRA) for health information technology and exchange which CHHS carried out through CalOHII and obtained the Office of the National Coordinator's (ONC) approval of the state's health information exchange strategic and operational plans. CalOHII is tasked with the management of the ARRA fund awarded to CHHS. Through the four-year cooperative agreement between CHHS and ONC, CalOHII will utilize $38.8 million in ARRA funds to enable electronic health information exchange across the state of California.

Meanwhile, the California Health Information Technology Act also authorized the Governor to designate a qualified nonprofit entity to be the state-designated entity for the purposes of health information exchange, pursuant to requirements as set in ARRA. In spring of 2010 Cal eConnect was selected as the state-designated entity and contracted by CalOHII through the ARRA fund to achieve the following requirements of the California Health Information Technology Act:

- Facilitate and expand the use and disclosure of health information electronically among organizations according to nationally recognized standards and implementation specifications while protecting, to the greatest extent possible, individual privacy and the confidentiality of electronic medical records.
- Develop strategic and operational plans to ensure that health information exchange capabilities are available, adopted, and utilized statewide so that patients do not experience disparities in access to the benefits of this technology by age, race, ethnicity, language, income, insurance status, geography, or otherwise.

California Health Information Organizations

California's existing health information exchange infrastructure is in various stages of development as multiple uncoordinated health information exchanges have developed over the past 15 years as regional initiatives. In the absence of a statewide health information exchange and while Cal eConnect follows its course of action, the existing and emerging health information organizations (HIO) are on the forefront of

interoperability as they endeavor to support community health care and improve care for the underserved. Below is a list of the current operational HIOs throughout California.

- Eastern Kern County Integrated Technology Association (EKCITA), www.ekcita.org
- Health Access El Dorado (ACCEL), www.acceledc.org
- Redwood MedNet, www.redwoodmednet.org
- Santa Cruz Health Information Exchange, www.santacruzhie.org/wp
- Western Health Information Network (WHIN), www.whinit.org/

In addition to these HIOs, there are integrated delivery networks (IDNs) that are currently operational within California, exchanging electronic health information within their organizations. Examples of these IDNs are Sutter Health and University of California, Davis, each which exchange data both within and between their respective organizations. Kaiser Permanente is also an example of an IDN that exchanges data between their many medical office buildings within their organization, as well as intra-organizationally with the Veterans Administration.

Summary /Overview of Demonstration Projects

On September 23, 2010, Governor Schwarzenegger approved AB 278 (Appendix M: Assembly Bill 278: Health Information Exchange: Demonstration Projects) which authorizes CalOHII to establish and administer demonstration projects for the electronic exchange of health information. These demonstration projects will be executed to evaluate potential solutions to facilitate health information exchange that promotes quality of care, respects the privacy and security of health information, and enhances the trust of the stakeholders. Demonstration projects will allow California to test privacy and security policy that will increase the trust of HIE participants by elevating protection of health information through innovative technology and sound business practice.

AB 278 authorizes CalOHII to approve up to four demonstration projects annually in order to address barriers to HIE implementation, test potential security and privacy policies, and identify differences between state and federal laws. The demonstration projects will test the following items as they enable exchange of electronic health information while increasing privacy protections:

1. Privacy and security policies and practices
2. New technologies
3. Implementation issues encountered by small health care practitioners

The bill also authorizes CalOHII to adopt regulations, to ensure all demonstration project participants follow a set of rules that frames the project and supports objectives. Regulations have been proposed and vetted twice among California health care industry stakeholders and will be finalized and filed with the Secretary of State for use by the demonstration project Participants.

On April 8, 2011, two demonstration projects were selected for 2011: Western Health Information Network (WHIN) and San Diego Beacon eHealth Community. These two projects will test privacy and security policies as set by the regulations and the demonstration project objectives.

WHIN Overview

WHIN is the only operational, community-based metropolitan HIO located in Los Angeles, and one of the largest Health Information Organizations currently operating in California with more than 500,000 unique patient IDs in a community master patient index. WHIN has a strong relationship and is a trusted partner for many healthcare delivery organizations in the Los Angeles and Orange Counties, and has been a leader in the protection of privacy and security since its inception in October, 2003. WHIN has been a participant in the efforts of the California Privacy and Security Advisory Board (CalPSAB), CalOHII, and the Nationwide Health Information Network, and has already implemented many proactive HIE protections, such as an Opt-In policy for access to health information by healthcare providers.

WHIN will be testing the Opt-In policy, including consent forms and education materials. As part of the project, WHIN will create patient-friendly videos that educate Californians on the benefits and risks of electronically exchanging health information in California. WHIN will collect specific data through the demonstration projects that will help inform whether the Opt-In policy is a viable option for California. Analysis of the data will identify barriers and assist in moving closer to optimal policy.

SD Beacon Overview

The San Diego Beacon Community is currently under development to link patients, health care providers, ambulances, clinics, and hospitals electronically to improve communication and share medical information important for the best medical care to all San Diegans. The San Diego Beacon Community includes the only academic medical school in the region (UC San Diego Health System), two large health systems in San

Diego County (Scripps Health and Sharp Healthcare), the only pediatric hospital (Rady Children's Hospital of San Diego), the VA Medical Center, Naval Medical Center, and all Federally Qualified Health Center clinics in the San Diego community. Additional partners include the County Public Health Department, San Diego City Emergency Medical Services agency, California Institute for Telecommunications and Information Technology, and San Diego State School of Public Health.

The San Diego Beacon Community will also be testing the Opt-In policy, including consent forms and education materials. The San Diego Beacon Community brings a different operational model for the Opt-In policy than the WHIN project and will assist in providing a broader policy perspective.

In November 2011, the San Diego Beacon Community was certified by the Office of the National Coordinator (ONC) and became an active participating organization on the Nationwide Health Information Network (NwHIN). San Diego Beacon Community is one of the first Beacon Communities on NwHIN, a milestone that was recently announced at the ONC Annual Meeting in Washington DC. San Diego Beacon Community will be joining other organizations such as the Veterans Affairs, Department of Defense, Social Security Administration and others to securely exchange patient health information on the NwHIN platform.

Demonstration Projects for the Electronic Exchange of Health Information

As authorized by AB 278, CalOHII may establish and administer demonstration projects funded by federal grants and other sources. The demonstration projects are to do all of the following:

(1) Identify barriers to implementing health information exchanges.
(2) Test potential security and privacy policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information.
(3) Identify and address differences between state and federal laws regarding privacy of health information.

Additionally, as authorized, CalOHII will adopt regulations to ensure that all approved demonstration project participants follow consistent rules and work within those parameters as they are engaged in the exchange of health information.

CalOHII has selected above two demonstration projects in 2011 for the electronic exchange of health information. These organizations will be the first Participants of such demonstration projects to be established in California.

Both the San Diego Beacon eHealth Community and WHIN will be able to test privacy and security policies across a broad spectrum of health care stakeholders. It is necessary for health systems to work together in order to compile the complete experience of a patient's care and ensure accessibility of that information to clinicians as the patient moves through various health care settings. The demonstration project Participants will support clinicians in making cost-effective, fact-based decisions that will reduce medical errors, decrease redundant tests and improve care coordination with the timely access to their patients' data.

One of the most important elements in creating an interoperable electronic exchange of health information for the demonstration projects is patient consent. It is important to emphasize that consent policies must be accompanied by privacy and security protections relating to authentication, authorization, access controls and auditing to earn patient trust. The consent must also satisfy all federal and California laws and regulations. The research and recommendations included in this document are a starting point for the comprehensive privacy and security policies that will be recommended by CalOHII for the demonstration projects.

Demonstration project Participants will be testing privacy and security policies for the electronic exchange of health information that will not only address the feasibility of implementation and gauge the implementation impact, but could identify needs for standardization across all participating health care entities as the Participants gauge the impact of the policies. Participation in the demonstration projects will provide the Participants with clarification on privacy and security issues, protection and mitigation of legal risks, and the structure to facilitate valuable and appropriately safeguarded testing of policies within the demonstration projects regulations. This will allow the Participants to be engaged in the advanced electronic exchange of health information environment in California as the State looks to the future.

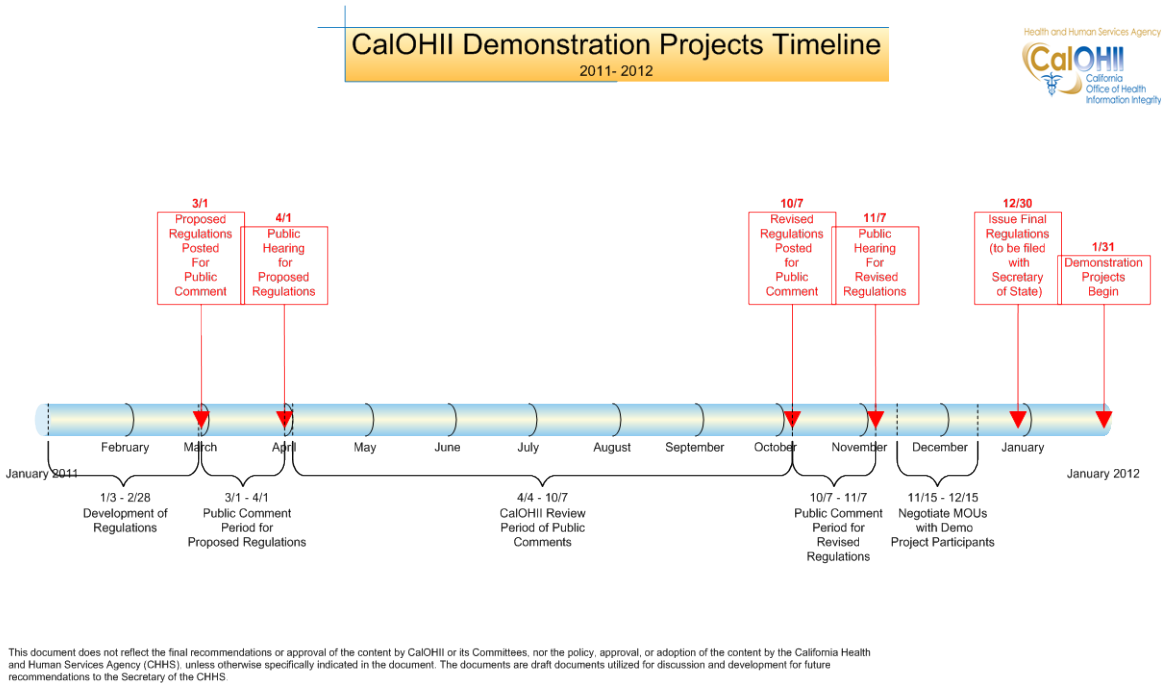
The demonstration project Participants will be informing CalOHII and HIE stakeholders on the critical privacy and security policy issues and identifying new and innovative privacy and security practices. Results from the demonstration projects will inform the California legislature of the outcomes, best practices, and the need for harmonization with federal privacy and security law.

The entire text of the Statement of Reasons and Regulations can be found in the appendices of this paper.

Summary of Demonstration Project Regulations/Statement of Reasons

This section will be written once the demonstration project regulations have been finalized and filed with the Secretary of State.

Demonstration Project Timeline



The table below depicts the historical development of the demonstration projects which is categorized into five phases of activities. Within each phase, the key accomplishments are listed.

Phase I: January 2010 to September 2010
• CalOHII drafts legislative proposal language for authority to establish and administer demonstration projects for the electronic exchange of health information • Assembly Bill 278 (Health information exchange: demonstration projects) is

introduced in California Assembly

- California Senate and Assembly committees and floor review, issue analysis, and conduct hearings
- Assembly Bill 278 is signed by the Governor and then chaptered: AB 278 (Chapter 227), an act to add and repeal Division 109.6 (commencing with Section130275) of the Health and Safety Code, relating to health information.

Phase II October 2010 to April 2011

- CalOHII issued a Request for Information in November 2010 to receive information from interested parties in the demonstration project(s)
- CalOHII issued the Request for Applications for the demonstration projects for the electronic exchange of health information in February 2011
- Concurrently, in February 2011, the Privacy Steering Team formed the Patient Consent and Informing Task Group and the task group begins its work on developing an opt-in consent form and informing document. Simultaneously, the Privacy Steering Team also formed the Secondary Use and Disclosure Task Group to begin addressing the potentially inappropriate secondary uses and disclosures of data.
- CalOHII issues the proposed demonstration projects regulations and the initial statement of reasons for public comments on March 1, 2011. These documents can be found at the links below.
  - Notice of Proposed Regulations
  - HIE Demonstration Projects Proposed Regulations - Text
  - Initial Statement of Reasons
  - Reference Documentation
- Public comment period for the revised demonstration projects regulations closed on April 1, 2011.
- CalOHII announced the two demonstration projects in April 2011.

Phase III April to September 2011

- CalOHII begins review and analysis of the one hundred eight plus public comments received on the proposed regulations
- CalPSAB is eliminated via the Governor's May Revise budget and the stakeholder structure of committees and task groups interact with CalOHII directly
- CalOHII aims to issue the revised demonstration projects regulations for a second public comment period by late 2011

Phase IV October 2011

- CalOHII issues the revised demonstration projects regulations and the revised statement of reasons for public comments on October 7, 2011. These documents can be found at the links below or in the noted Appendices.
  - Demonstration Projects Notice of Revised Regulations (Appendix D: Demonstration Projects Notice of Revised Regulations).
  - Revised Demonstration Projects Regulations (Appendix E: Revised Demonstration Projects Regulations)
  - Revised Statement of Reasons (Appendix F Revised Statement of Reasons)
  - Revised Demonstration Projects Reference Documentation (Appendix G: Revised Demonstration Projects Reference Documentation)
- Final demonstration project regulations to be filed with the Secretary of State -- TBD

The two demonstration project Participants to use the consent form and informing document developed by the Patient Consent and Informing Task Group and as approved by the Privacy Steering Team and CalOHII.

Oversight and Audits

The auditing provisions, including examples of information which may be inspected, are intended to allow CalOHII to verify the information provided in the demonstration project

application and the eventual agreement. CalOHII does not intend to inspect all parts of a Participant's operations, only those related to the exchange of health information within the scope of the demonstration project. The process is intended to allow for flexibility in compliance auditing, ranging from inspecting the requested documentation to an onsite inspection of the operations of the Participant, including requested documentation. If a Participant is believed to be in non-compliance, CalOHII will request documents or other information concerning the possible non-compliance.

Demonstration Project Metrics

As stated earlier on pages 18 and 19 of this paper, per AB 278, "It is the intent of the Legislature that the demonstration projects do all of the following:

(1) Identify barriers to implementing health information exchanges.

(2) Test potential security and privacy policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information.

(3) Identify and address differences between state and federal laws regarding privacy of health information".

To best comply with this legislation, CalOHII will utilize an independent auditor to objectively and efficiently evaluate the demonstration projects. To best prepare the metrics to be used for this evaluation, CalOHII developed an initial list of metrics that was then vetted and further developed by the expertise of the Patient Consent and Informing Task Group. This list of metrics will be refined with the independent evaluator to assist with a meaningful evaluation of each of the demonstration projects. The draft form of the metrics document can be found in Appendix H: Demonstration Project Metrics Document.

The next section will discuss the opt-in consent policy that the demonstration project Participants will be utilizing.

Opt-in Consent Policy

The choice of requiring affirmative consent reflects discussion and consideration of the topic since 2008. Through meetings, research, and various alternate proposals, a broad cross section of the health care community recognized that there were numerous privacy, legal, technological limitations and implementation issues with each of the possible approaches to consent. This finding has been echoed on the Federal level

with the work of the Health Information Technology Policy Committee of the Office of the National Coordinator.

Electronic health information exchange presents an unprecedented possibility of broad exposure of health information that is protected by both Federal and State privacy laws. While there has always been a risk of unauthorized access, electronic medical records in a network exponentially expands the potential consequences of unauthorized access to medical records. The interconnectedness envisioned of electronic health information exchange would allow potential access to numerous records, and portions of records, that might otherwise be inaccessible. Health information that may be considered particularly sensitive, and sometimes protected by law, may be contained within an accessible record beyond the need for treatment (think of a podiatrist having access to alcohol treatment records). It should also be noted that in comparison with paper-based records, the use of electronic health records and electronic exchange of health information which allow for authentication protocols, encryption, etc., could positively contribute to the quality of care while improving the outcome for the patient.

The possibility of unintended, overly broad, and unnecessary disclosures due to the lack of technological capability to segment data weighs in favor of an affirmative consent policy. The President's Council of Advisors on Science and Technology report states (page 4) that "the indexing and retrieval of a metadata-tagged data, across large numbers of geographically diverse locations, is an established highly developed technology" and continues to state that "With ONC leadership, these technologies could rapidly be adapted and standardized for universal use in health IT. Innate, strong, privacy protection on all data, both at rest and in transit, with persistent patient-controlled privacy preferences, is likewise achievable, and must be designed in from the start". One way of having persistent patient-controlled privacy preference is providing the patient with the right to consent. In addition, there are several state laws requiring the special treatment and protection of sensitive health information such as HIV test results, psychotherapy notes, lab results, and genetic testing. A listing of these laws can be found in Appendix I: California Law: Confidentiality and Disclosure Chart.

Continuing with the consent policy research work completed by CalPSAB and the opt-in consent policy recommendation that was forwarded to the Secretary, California Health and Human Services, the Privacy Steering Team created the Patient Consent and Informing Task Group in January 2011. The purpose of this task group was to refine the policy recommendation and develop implementation guidance through the development of a patient consent form and informing material. However, CalOHII believes that the reading of an informing document and the signing of a consent form is the step at the end of a process – the process of education. The education of the patient on the various aspects of the electronic exchange of health information, is to guide the patient in making a meaningful decision in giving or not giving his/her consent.

Therefore, CalOHII is developing an educational webpage for patients and providers in order to assist both in making informed decisions as it relates to the electronic exchange of health information. Further information about CalOHII webpage for patient and provider educations is available on pages 27- 29 of this document.

By requiring a patient to give affirmative consent in conjunction with an educational component before their health information is exchanged electronically, the risk to the participants in a health information exchange system is minimized. Given the potential liability for violation of privacy, and the technological limitations of the current electronic medical records and health information exchanges, an affirmative consent policy was adopted. The various references reviewed in the development of this consent policy can be found in Appendix B: References and Appendix J: Other States' Consent Model.

Consent Policy Discussion

The current laws that govern health information exchange were developed in a paper-based world where the decisions regarding what, how and to whom to communicate were generally made on a one-to-one basis by clinicians and their patients. These current laws serve the patient's privacy interests by restricting what can and cannot be shared, and the terms which sharing takes place. Human judgment and personal relationships play a major role in information exchange decisions.

As previously stated, moving from a paper to an electronic health system changes the information-sharing dynamic. The demonstration projects will facilitate a many to many relationship among providers, enabling different information technology systems and software applications to exchange information accurately, effectively and consistently. This offers new opportunities to promote access to health care information, as well as to facilitate the safety, quality and efficiency of health care.

The all or none opt-in patient consent which will be tested by the demonstration projects for the electronic exchange of health information, in conjunction with the informing document and the patient education component, provides the patient the opportunity to make a meaningful decision at the front end on whether their health information should flow or not. Patients could have many reasons such as religious, cultural, or personal for not wanting their health information or medical information to be exchanged electronically or otherwise. The opt-in consent allows the patient to exercise their right to privacy at the front end.

Each Participant in the current demonstration projects must obtain an affirmative consent from the patient that specifically references the demonstration projects prior to accessing his/her electronic health information.

Requiring patients to consent to the exchange of their information for the demonstration projects ensures that they know how their information will be shared and used among the demonstration project Participants. It also lets patients decide whether to allow their information to be shared and used in this manner. Thus, the use of the Patient Consent form promotes openness and transparency and stimulates patient choice as recommended by the ONC Tiger Team.

Exceptions to Consent

Public Health Reporting

There are required reporting obligations on health care providers to submit health information to public health officials. Because these are required by law, the patient is not being given the opportunity to consent to these types of disclosures through a HIE. The demonstration projects could showcase the privacy and security features of these types of exchanges, the risk of inappropriate secondary use of the information will be negligible and the transparency and security features will help to build trust. Meanwhile, the Secondary Use and Disclosure Task Group has drafted a recommendation to the Privacy Steering Team that allows health care providers to electronically submit data through a health information exchange to public health agencies for purposes of mandatory public health reporting.

Break the Glass

Certain emergency situations inhibit a provider from obtaining affirmative consent prior to accessing the electronic health records of an individual. In qualifying situations, the medical provider may access the electronic health records of an individual without the individuals' prior affirmative consent. This policy balances the needs of the health care provider to have information related to the individual with the privacy rights of the individual. By allowing access to an individual's records in an emergency situation, within set parameters, unless the individual has previously withheld or withdrawn their consent to electronically exchange their health information, the health care providers need for information is supported without undermining the privacy rights of the individual.

Patient Education

The proposed demonstration project regulation specifies that certain general information must be provided to the individual prior to the individual granting consent to electronically exchange their Individual Health Information (IHI). In order for consent to be meaningful, an individual must be informed of certain information on which to make an educated decision. The notion of meaningful consent is foundational in most iterations of Fair Information Practice Principles. Both the CalPSAB principles as well as the Federal Privacy and Security Tiger Team recommendations recognize the need for meaningful consent.

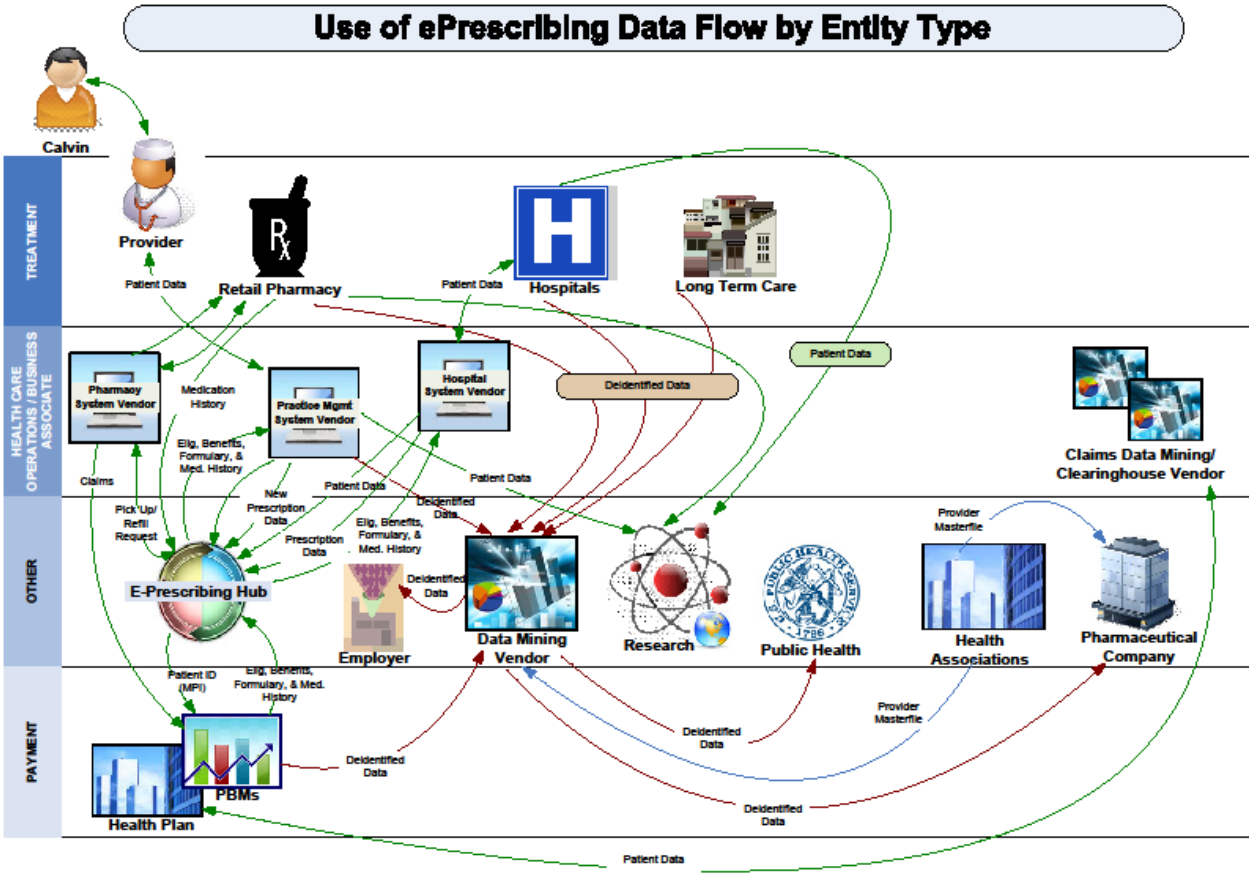
The information provided to the individual before consent may be given reflects both substantive and procedural information necessary for an informed choice. Given that electronic health information exchange is a new field, few people outside the field are aware of the potential benefits and risks in electronically sharing IHI. By providing substantive explanations of the way electronic health information exchange works, the uses of the data once exchanged, and the accompanying benefits and risks, the individual will be educated in a transparent process. The regulations do not require specific formulations of words, to allow flexibility for different organizations to provide different accounts of the ways the information is used, exchanged, and the benefits and risks specific to their organization.

The regulations are purposely silent on the specific language to use in these descriptions, so that various approaches may be tested for effectiveness and fulfill the obligation to test privacy policies under AB 278. Additionally, each organization will have a different system of electronic exchange so allowing flexibility is appropriate within basic parameters.

Currently and as promulgated by the Tiger Team, the responsibility of educating and informing the patients of their privacy rights and the use of their health information is mostly the responsibility of the physician, so is the protection of the patients' health information. However, as electronic health records (EHR) are established and utilized, and as HIEs and HIOs operated by vendors become commonplace, in the future the responsibility could become a shared one.

The data flow diagram below, Diagram 1. Use of ePrescribing Data Flow by Entity Type, is an illustrative example of the data flow triggered by a patient obtaining a prescription from his/her physician, and the various places and entities where the information could go through the electronic exchanges. The demonstration projects' patient education process should foster patients' increased understanding of to whom their data is going and for what purpose.

Diagram 1: Use of ePrescribing Data Flow by Entity Type



The importance of the patient education process was addressed by the Patient Consent and Informing Task Group and the list of suggested methods to facilitate the patient education process was compiled. As stated above, while flexibility within each demonstration project's organization is preferred, the list below is not intended to be prescriptive, but a suggestion of possible methods that may prove successful in the variety of patient populations within the demonstration projects.

- Informing material – The informing document that the Patient Consent and Informing Task Group and CalOHII developed collaboratively. This document can be found in Appendix K: Patient Informing Material.
- Communication Plan – branding and logo-recognizable by the time patient gets to his/her provider

- Social Media – Facebook and Twitter, Cartoon character recognizable by the time the patient gets to his/her provider
- Public Service Announcements
- Software demonstrations – Explaining how patient would interface with electronic health information exchange system, why do this? Why do we care? Demo video (multi-media) like slides but interactive
- Flow charts and visual aids – Available at a variety of places throughout the community such as: provider offices, libraries, hospitals, pharmacies, etc. The materials should be available in population-appropriate languages and cultures and observe
- Frequently Asked Questions (FAQs)
- CalOHII Patient and Provider Education webpage

Consent Form

The demonstration project Participants will utilize a CalOHII-approved consent form to obtain and document the affirmative patient consent of its patients. The Patient Consent Form can be found in Appendix L: Patient Consent Form.

The Patient Consent form includes the elements identified in Table 2: Patient Consent Form Requirements.

Table 2: Patient Consent Form Requirements

The Patient Consent form required to be signed for a physician to access a patient's individual health information record by the demonstration project Participants will include the following elements: • The information to which the patient is granting the Participant access • The intended uses of the information by the Participant • The relationship between the Participant and the patient whose information will be accessed • Certification that only those engaged in the intended uses may access the patient's information • Acknowledgement of the patient's right to revoke consent and assurance that treatment will not be affected as a result • Whether and to what extent information is subject to re-disclosure; information may be re-disclosed unless prohibited by state or federal law • The consent will be valid until the patient chooses to revoke • The signature of the patient or the patient's authorized representative • The date of execution of the consent • Reference to all demonstration project Participants at the time of the patient's consent, as well as an acknowledgement that HIE participants may change over time and instructions for patients to access an up to date list of demonstration project Participants through the health care provider's office or website

Durability and Revocability

The duration of the patient consent will be determined by the demonstration project Participants. The recommendation set forth in the Patient Consent form allows the consent to remain in effect until the patient revokes his/her consent.

An individual or the individual's personal representative may revoke their previously granted consent to the electronic exchange of health information by contacting the designated contact person or entity as described in the Patient Consent form. After the effective date of the revocation of consent, the demonstration project Participant shall not allow the individual's individual health information to be electronically exchanged unless and until the individual or the individual's personal representative reinstates consent.

Appendix A: Terms and Definitions

Authorization – The documentation from a patient or their representative in accordance with various laws regarding the need for a special permission or an authorization for the use and disclosure of individual health information. An authorization under these provisions means an authorization in the form required, depending on the outcome of a participant's HIPAA preemption pursuant to 45 CFR 160.203, that is in compliance with Civil Code sections 56.11, 56.21; Insurance Code section 791.06, and/or 45 CFR 164.508 or as required by more stringent law.

Break the Glass - The ability of a health care provider, in the case of an emergency to access a patient's individual health information without obtaining the patient's consent.

Business Associate Agreement - A contract or other arrangement between a HIPAA covered entity and its business associate, required by HIPAA (45 C.F.R. §164.308(b)), that specifies the permitted uses and disclosures of individual health information, requires the use of appropriate safeguards to prevent the use or disclosure of the individual health information other than the permitted purposes specified in the agreement, and details the scope of any other responsibilities.

California Privacy and Security Board (CalPSAB) - California Privacy and Security Advisory Board (CalPSAB) provided private and public collaboration to address and coordinate health information exchange (HIE) privacy and security efforts in California. The CalPSAB's three committees: Privacy, Security and Legal analyzed issues, developed and evaluate the effectiveness of alternative solutions, and presented recommendations to the CalPSAB. The CalPSAB reviewed and approved their recommendations, and presented approved recommendations for consideration by the Secretary of the California Health and Human Services Agency.

Consent - An express permission given by a patient for the exchange of his or her personal health information through an HIE in response to a clear and specific request for such permission or at the individual's own initiative.

Demonstration Project Participant - A health care entity, health care service plan or health information organization approved by CalOHII to test privacy and/or security policies for the exchange of electronic health information.

Electronic Health Record (EHR) - The definition given at section 13400 of subtitle D of the American Recovery and Reinvestment Act of 2009: "an electronic record of health-related information about an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

Health Information Exchange (HIE) - A health information system that can electronically disclose health information outside the Participant holding the information.

Health Information Organization (HIO) - A third party facilitator that conducts, oversees, or governs the disclosure of individual health information among separate, unaffiliated entities.

ONC - Office of the National Coordinator for Health Information Technology at the Department of Health and Human Services.

Patient Consent Form - The form that must be read and signed by a patient before any demonstration project Participant can access that patient's health records through the HIE. This consent is the floor of consent in the state of California for exchange of information for treatment and payment and is a more thorough consent than that required by HIPAA.

Sensitive Health Information – Legally and traditionally recognized categories of sensitive information, such as genetic information, mental health, substance abuse treatment, HIV-related information, sexuality and reproductive health or specific segments of a patient's individual health information for which a patient has expressed their privacy concerns.

Appendix B: References

The following references were reviewed during the consent policy development process.

Federal references:

1. **Executive Office of the President: President's Council of Advisors on Science and Technology Report**
   Report to the President: Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward
   http://www.whitehouse.gov/administration/eop/ostp/pcast/docsreports

2. **Federal Trade Commission Report**
   Protecting Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policy Makers
   http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

3. **National Committee on Health and Vital Statistics Recommendations**
   Letter to the Secretary, U. S. Health and Human Services Agency: Recommendations Regarding Sensitive Health Information:
   http://www.ncvhs.hhs.gov/101110lt.pdf

4. **ONC Tiger Team Recommendations**
   The HIT Policy Committee has made recommendations to the National Coordinator on privacy and security policies and practices. The recommendations, from the Privacy & Security Tiger Team, were approved by the HIT Policy Committee during its August 19, 2010, teleconference call. The HIT Policy Committee recommendations have been transmitted to the National Coordinator.

   http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_6011_1815_17825_43/http%3B/wci-ubcontent/publish/onc/public_communities/_content/files/hitpc_transmittal_p_s_tt_9_1_10.pdf

CalOHII references:

Link to White Paper: ANALYSIS OF THE RISKS Inherent in Implementing HIE Services & Strategies on How to Proceed in the Development of HIE Policies and Standards.

http://www.ohi.ca.gov/calohi/LinkClick.aspx?fileticket=Adh9MKWj0RU%3d&tabid=36

Appendix C: CalPSAB Letter to Secretary Dooley

CALIFORNIA PRIVACY AND SECURITY ADVISORY BOARD

January 13, 2011

Secretary Diana Dooley
California Health and Human Services Agency
1600 Ninth Street, Room 460
Sacramento, California 95814

Re: Consumers Union & Center for Democracy & Technology Request for Reconsideration of CalPSAB Consent Decision

Dear Secretary Dooley:

Welcome to California Health and Human Services Agency. As co-chairs of the California Privacy and Security Advisory Board (CalPSAB), we look forward to continuing to assist your office in developing privacy and security standards for health information exchange (HIE) in California.

By way of background, on September 30, 2007, CHHS Secretary Kimberley Belshé established the CalPSAB and made the appointment of a variety of healthcare stakeholders and consumer representatives to this Board. The charge was for CalPSAB to oversee and coordinate a statewide collaborative process to identify privacy and security standards and policies necessary for the safe exchange of electronic health information in California.

The mission of CalPSAB is to develop and recommend these privacy and security standards for HIE to promote quality of care, respect the privacy and security of personal health information, and enhance trust. The strategic approach has been to utilize a combination approach of addressing issues from the specific project scenario perspective. For example, an analysis should consider a national use case and a local HIE effort in unison to create a scenario for which to analyze the issue.

On the issue of consent, we began work on this issue in 2008 working on four use case scenarios. In the development of the initial set of guidelines, we focused on whether affirmative consent should be included. After numerous meetings and consideration of diverse proposals, in October 2010 the Board had reached a decision. Subsequent to that

decision, inquires were made to the former Secretary Kimberley Belshé and she requested that the Co-Chairs of California Privacy and Security Advisory Board (CalPSAB) consider the request by Consumers Union (CU) and the Center for Democracy & Technology (CDT) regarding the federal Privacy and Security Tiger Team (Tiger Team) recommendations.

In the interest of transparency, the entire CalPSAB met on December 9, 2010 to permit a full discussion of the Tiger Team recommendations, their development, and their authority. The 2 ½ hour discussion provided a solid foundation to compare and contrast the CalPSAB guidelines and Tiger Team recommendations. Board members actively engaged with the representatives from CU and CDT to try to gauge the best policy choices in the California context. At the conclusion of the meeting, Board members were asked to submit written comments outlining their concerns or reasoning if they thought the CalPSAB consent decision should be reconsidered in light of the discussion. We received no such requests or comments.

The clear take away from the discussion was the difference in focus between CalPSAB and the federal Privacy and Security Tiger Team. In 2007, CalPSAB was charged with developing privacy and security standards and policies necessary for the safe and secure exchange of electronic health information in California. The Tiger Team's charge is limited to meeting the privacy and security needs for those seeking government incentive money for meeting the criteria in Stage 1 of Meaningful Use, a very small subset of exchange situations.

Because the exchange situations of the Tiger Team are a subset of the exchange situations considered by the CalPSAB, the two proposals are very similar. Both were developed in a public process, the Tiger Team utilizing a board over a three month period this summer, and CalPSAB utilizing a board of California healthcare stakeholders, task groups, surveys, and multiple public comment periods from July 2009 to October 2010. Both sets of recommendations explicitly state they will require further development over time. The Tiger Team recommendations must be expanded beyond the narrow confines of Meaningful Use Stage 1 and the CalPSAB guidelines will be revised as policy and implementation issues are identified and resolved through testing in demonstration projects.

In September 2009, CalPSAB recommended a bifurcated consent policy: opt-out for treatment and opt-in for other purposes or if particularly sensitive information was included in the medical record. The public was requested to comment on this proposal. The public comments received from 33 organizations and 1,232 individuals made it clear that nearly all of the healthcare stakeholders thought the bifurcated policy could not be made operational in a cost effective manner, and the patients did not find it satisfactory in protecting their privacy. Based on the nearly unanimous rejection of the proposed bifurcated consent policy, the CalPSAB withdrew the recommendation in December 2009 and began working again towards a consensus position.

The Tiger Team proposal is bifurcated similar to the recommendation withdrawn by the CalPSAB in January, yet is less protective of privacy: no patient consent for direct exchange for treatment and an undefined consent if certain triggering events were to occur, such as use of a Health Information Organization to facilitate the exchange of information, etc. This does not allow the patient to opt-out of electronic exchange and does not define how consent, when needed, is to be implemented.

Subsequent to the CalPSAB meeting in December 2009, various scenarios and concerns were discussed, such as the practicality of the recommendation in an emergency room, and possible implementation issues. The final CalPSAB consent policy reflects a decision that was satisfactory to nearly all parties. It may not have been what each party hoped the policy would be, but it is one they can implement successfully in the current technological, legal and political environment.

CalPSAB represents a wide range of California healthcare stakeholders, including consumers, who sought additional information from their respective stakeholders in reaching a consensus position on consent. While the Tiger Team recommendations have some useful elements, especially considering the similarities with the CalPSAB guidelines, they do not represent the results of a California stakeholder process. We have heard the Tiger Team recommendations and have decided they are not the best long term solution for the healthcare community in California. We therefore stand by our recommendation from the October 12, 2010 CalPSAB meeting, and advise the adoption of a policy requiring affirmative patient consent before the electronic exchange of health information.

While we understand that we work on CalPSAB at your pleasure, we believe that there is much more work to be done. We would like to continue our work to assist in resolving these perplexing policy issues. CalPSAB has worked as a good forum for the development and dialog on these issues within a constructive, inclusive, and well defined process.

Sincerely

Pam Dixon
Executive Director
World Privacy Forum
& CalPSAB Co-Chair

William Barcellona
Vice President for Governmental Affairs
California Association of Physician Groups
& CalPSAB Co-Chair

Cc: Dr. Linette Scott,
Interim Deputy Secretary for HIT

Appendix D: Demonstration Projects Notice of Revised Regulations

Division 14 California Office of Health Information Integrity

Chapter 1 HIE Demonstration Projects

Notice of Proposed Regulations

The California Office of Health Information Integrity (CalOHII) proposes to adopt regulations described below after considering all comments, objections, and recommendations regarding the proposed action.

PUBLIC HEARING

CalOHII will hold a public hearing on Monday, November 7th, 2011 at the following location:

California Department of Social Services
Office Building #8 – Room 235/237
744 P Street
Sacramento, California, 95814

The public hearing will convene at 9:00 am, and it will remain open only as long as attendees are presenting testimony. Attendees must check in at the security desk to receive a visitor's badge. The purpose of the hearing is to receive public testimony, not to engage in debate or discussion. The hearing will adjourn immediately following the completion of testimony presentations.

WRITTEN COMMENT PERIOD

Any interested person, or his or her authorized representative, may submit written comments relevant to the proposed regulatory action to CalOHII. The written comment period closes at 5:00pm on Monday, November 7th, 2011. CalOHII will consider only comments received at the CalOHII office or by email by that time. Submit comments to:

Staci Gillespie
CalOHII
1600 9th Street, Room 460
MS 20-10
Sacramento, CA 95814
(916)651-3364

sgillespie@ohi.ca.gov

AUTHORITY AND REFERENCE

Assembly Bill 278, codified at California Health and Safety Code § 130275 et seq, authorizes CalOHII to establish and administer demonstration projects to test privacy and security policies for health information exchange in California. As part of AB278, CalOHII is authorized to adopt regulations for the demonstration projects to ensure all participants follow consistent rules.

INFORMATIVE DIGEST/POLICY STATEMENT OVERVIEW

Assembly Bill 278 (Stat. 2010 Ch. 227 (Monning); codified at Health and Safety Code § 130275 et seq.) authorizes the Director of the California Office of Health Information Integrity (CalOHII) to approve demonstration projects for electronic health information exchange (HIE). CalOHII has the general authority to enforce state laws mandating the confidentiality of medical information. These projects will test policies and rules to better inform the state and healthcare stakeholders while the HIE infrastructure is being defined over the next several years. By allowing for various HIE demonstration projects, it will be possible to determine how best to protect privacy in accordance with state and federal laws while enabling electronic health information exchange.

Pursuant to California Health and Safety Code § 130277, the Director of CalOHII may adopt regulations applicable to demonstration projects and health care entities voluntarily using the health information exchange services developed according to the instant division of law. The Director was granted this authority to ensure that testing potential privacy and security policies occurs within acceptable parameters and the parties involved follow the same basic rules.

DISCLOSURES REGARDING THE PROPOSED ACTION

Mandate on local agencies and school districts: None.

Cost or savings to any state agency: None.

Cost to any local agency or school district which must be reimbursed in accordance with Government Code sections 17500 through 17630: None.

Other nondiscretionary cost or savings imposed on local agencies: None.

Cost or savings in federal funding to the state: None.

Significant, statewide adverse economic impact directly affecting business including the ability of California businesses to compete with businesses in other states: None.

Cost impacts on a representative private person or businesses: None.

Significant effect on housing costs: None.

Adoption of these regulations will not: None.

(1) Create or eliminate jobs within California
(2) Create new business or eliminate existing businesses within California; or
(3) Affect the expansion of businesses currently doing business within California.

CONSIDERATION OF ALTERNATIVES

AB 278 provides CalOHII an exemption from the requirements of the Government Code section 11346.7, subdivision (a)(13). Nevertheless, CalOHII will consider alternatives and determine that no reasonable alternative it considered or that has otherwise been identified and brought to the attention of the agency would be more effective in carrying out the purpose for which the action is proposed or would be as effective and less burdensome to affected private persons than the proposed action.

CalOHII invites interested persons to present statements or arguments with respect to alternatives to the proposed regulations at the scheduled hearing on November 7th , 2011. CalOHII also will accept written statements or arguments during the written comment period which ends on November 7th, 2011.

CONTACT PERSONS

Inquiries concerning the proposed administrative action may be directed to:

Staci Gillespie
CalOHII
1600 9th Street, Room 460
MS 20-10
Sacramento, CA 95814
(916)651-3365
sgillespie@ohi.ca.gov

The backup contact person for these inquiries is:

Suzanne Giorgi
CalOHII
1600 9th Street, Room 460
MS 20-10
Sacramento, CA 95814
(916)651-3364

sgiorgi@ohi.ca.gov

Please direct requests for copies of the proposed text (the "express terms") of the regulations, the statement of reasons, the modified text of the regulations, if any, or other information upon which the rulemaking is based to Staci Gillespie or Suzanne Giorgi at the above addresses and phone numbers.

AVAILABILITY OF STATEMENT OF REASONS, TEXT OF PROPOSED REGULATIONS, AND RULEMAKING FILE

CalOHII will have the entire rulemaking file available for inspection and copying throughout the rulemaking process at its office at the above address. The rulemaking file consists of this notice, the proposed text of the regulations, reference documentation, and the initial statement of reasons. Copies may be obtained from the CalOHII website at: http://www.ohi.ca.gov/calohi or by contacting Staci Gillespie or Suzanne Giorgi at the addresses or phone numbers listed above.

AVAILABILITY OF THE FINAL STATEMENT OF REASONS

Upon its completion, copies of the Final Statement of Reasons may be obtained by contacting Staci Gillespie or Suzanne Giorgi at the above addresses and phone numbers.

AVAILABILITY OF DOCUMENTS ON THE INTERNET

Copies of the Notice of Proposed Action, the Initial Statement of Reasons, the text of the regulations in underline and strikeout, and the reference documentation can be accessed through the CalOHII website at:: http://www.ohi.ca.gov/calohi.

Appendix E: Revised Demonstration Projects Regulations

Title 22, Division 14
California Office of Health Information Integrity

Table of Contents

Division 14 California Office of Health Information Integrity

Chapter 1 ~~HIE~~ Demonstration Projects for the Electronic Exchange of Health Information

§126010 Applicability of Regulations

This document does not reflect the final recommendations or approval of the content by CalOHII or its Steering Teams, nor the policy, approval, or adoption of the content by the California Health and Human Services Agency (CHHS), unless otherwise specifically indicated in the document. The documents are utilized for discussion and development for future recommendations to CalOHII.

(a) The regulations in this chapter apply to ~~D~~demonstration ~~P~~project Participants ~~and Health Information Exchange Service Participants,~~ as defined in California Health and Safety Code §130276.

(b) Effective dates. The regulations adopted in this chapter will become inoperative on the date the CalOHII Director executes a declaration stating that the grant period for the State Cooperative Grant Agreement for health information exchange has ended and this chapter will then be repealed. ~~are effective on **[insert the date filed with secretary of state].**~~

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: California Health and Safety Code §§ 130276, 130277,130278, 130282.

§126020 Definitions

(a) "Access" means the HIPAA definition given at 45 C.F.R. §164.304.~~: ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any health information.~~

(b) "Affiliated entity" means legally separate entities who have designated themselves as a single, affiliated entity and are under common ownership or control.

~~(b)~~(c) "Applicant" means an entity that submits an application to CalOHII for approval as a ~~D~~demonstration ~~P~~project.

(d) "Authorization" as used in section 126055(b)(2) means the documentation from a patient or their representative in accordance with various laws regarding the need for a special permission or an authorization for the use and disclosure of individual health information. An authorization under these provisions means an authorization in the form required, depending on the outcome of a participant's HIPAA preemption pursuant to 45 C.F.R. §160.203, that is in compliance with Civil Code sections 56.11, 56.21; Insurance Code section 791.06, and/or 45 C.F.R. §164.508 or as required by more stringent law.

~~(c)~~(e) "Business Associate" means~~:~~ the HIPAA definition given at 45 C.F.R. §160.103.

~~(1) With respect to a health care provider, an entity on behalf of such health care provider, but other than in the capacity of a member of the workforce of such health care provider who:~~

~~(A) Performs, or assists in the performance of a function or activity involving the use or disclosure of identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or~~

~~(B) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such health care provider, where the provision of the service involves the disclosure of individual health information from such health care provider or from another business associate of such health care provider, to the person.~~

~~(2) A health care provider may be a business associate of another health care provider.~~

~~(d)~~(f) "Business Associate Agreement"

A contract or other arrangement between a ~~health care provider~~ HIPAA covered entity and its business associate, required by HIPAA (45 C.F.R. §164.308(b)), that specifies the permitted uses and disclosures of individual health information, requires the use of appropriate safeguards to prevent the use or disclosure of the individual health information other than the permitted purposes specified in the agreement, and details the scope of any other responsibilities.

~~(e)~~(g) "CalOHII" means the California Office of Health Information Integrity.

(h) "CMIA Provider" means the Confidentiality of Medical Information Act definition of a Provider of Health Care given at Civil Code section 56.05(j).

~~(f)~~(i) "De-identified health information" means the HIPAA definition given at 45 C.F.R. §164.514. ~~health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Compliance with federal standards for de-identification of health information, as codified 45 C.F.R. § 164.514, shall be deemed adequate for de-identified health information.~~

~~(g) "Direct exchange" means the electronic exchange or access to of health information without the use of a health information organization:~~

~~(1)Through a direct connection between the electronic health record systems of health care providers; or~~

~~(2)From a health care provider or entity to another health care provider or entity utilizing national or state standards, services, and policies including but not limited to the standards, services and policies of the Direct Project of the National Health Information Network.~~

(j) "Disclosure" means the HIPAA definition given at 45 C.F.R. §160.103.

~~(h)~~(k) "Electronic Health Record (EHR)" means the definition given at section 13400 of subtitle D of the American Recovery and Reinvestment Act of 2009: "an electronic record of health-

related information about an individual ~~and~~ that ~~can be~~ is created, gathered, managed, and consulted by authorized health care clinicians and staff."

~~(i) "Entity" means a person, corporation, association, partnership or other legal entity, other than an individual or the individual's personal representative in possession of health information pertaining to the individual~~.

(l) "EHR Vendor Agreement" means the document that specifies the contractual arrangements and licenses between the participant and the primary organization that provided the participant with their EHR system and/or provides on-going technical support for the participant's EHR system.

(m) "Governmental authority" means any municipal, county, state or other governmental entity that has jurisdiction and control over the provision or payment for medical services or that routinely received medical information to complete its designated governmental function, including specialized units from the local and state Public Health authorities.

~~(j)~~(n) "Health Care Provider" means the HIPAA definition given at 45 C.F.R. §164.103.~~: means a person or entity that is a health care provider under 45 C.F.R. § 160.103, or is a provider of health care under California Civil Code § 56.05(j).~~

~~(k) "Health Information" means any information, whether oral or recorded in any form or medium, that:~~

~~(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, health care clearing house, personal health record, health information organization, or any other entity; and~~

~~(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual~~

~~(l) "Health Information Exchange" (HIE) means the electronic movement or access to health information~~.

~~(m)~~ (o) "Health Information Organization" (HIO) means ~~an entity~~ a third party facilitator that conducts, oversees, or ~~and~~ governs the ~~exchange~~ disclosure of ~~or access to~~ individual health information among separate, unaffiliated entities.

(p) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 as amended by subsequent legislation and the implementation of Privacy, Security, and Enforcement Rules under 45 C.F.R. Part 160 and Subparts A, C, D, and E of Part 164.

(q) "HIPAA covered entity" means the HIPAA definition for covered entity given at 45 C.F.R. 160.103.

(r) "Independent Directed Exchange" means the electronic disclosure of encrypted individual health information over the internet to an unaffiliated entity and where third party facilitators do not have the ability to decrypt the content of the individual health information (IHI) package nor provide governance or oversight.

~~(n)~~(s) "Individual" means the person who is the subject of health information.

~~(o)~~(t) "Individual Health Information" (IHI) means ~~information about an individual that alone or in conjunction with other reasonably available information includes or relates to:~~
~~(1) Demographic information,~~
~~(2) The past, present, or future physical or mental health or condition of the individual~~
~~(3)The provision of health care to an individual, or~~
~~(4) The past, present, or future payment for the provision of health care to an individual.~~
information, in oral, electronic or physical form, including demographic information collected from an individual, and:

(1) Is created or received by or derived from a health care provider, health care clearinghouse, health plan, employer, pharmaceutical company, or contractor;
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(3) Is Individually identifiable which means the information includes or contains any element of personal identifying information to which there is a reasonable basis to believe the information can be used to identify the individual such as the patient's name, address, electronic mail address, telephone number, social security number, or other information that, alone or in combination with other potentially available information, reveals the individual's identity.

(u) "More stringent law" means: in the context of a comparison of a provision of State or federal law, including HIPAA, against another law, a "more stringent law" is one that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under another law or rule, except if the disclosure is
(A) Required by the federal Secretary of Health and Human Services in the context of HIPAA, in connection with determining whether a covered entity is in compliance with this subchapter; or
(B) To the individual who is the subject of the individual health information.

(2) With respect to the rights of an individual, who is the subject of the individual health information, regarding access to or amendment of individual health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individual health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individual health information, for use or disclosure of individual health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individual health information.

~~(p)~~ (v) "Participant" means ~~a demonstration project Participant~~ a provider, a health plan, a health information organization, or a governmental authority approved by CalOHII to test privacy and/or security policies for the exchange of electronic health information.

(w) "Participants Agreement" (PA) means a multi-party trust agreement among organizations exchanging health information that sets a common set of terms and conditions for the organizations establishing a mutual governance process amongst participants.

~~(q)~~ (x) "Public Health" This term refers to public health authorities whose public health programs promote, maintain, and conserve the public's health by providing health services to individuals and/or by conducting research, investigations, examinations, training, and demonstrations. ~~This definition is consistent with state and federal definitions of public health programs and as the term is used in the meaningful use incentive program.~~

(y) "Sensitive health information" means legally and traditionally recognized categories of sensitive information, such as genetic information, mental health, substance abuse treatment, HIV-related information, sexuality and reproductive health or specific segments of a patients individual health information for which a patient has expressed their privacy concerns.

~~(q) "Trading Partner" means an entity that has a Trading Partner Agreement with an Applicant or Participant for the exchange of information in electronic transactions.~~

~~(r) "Trading Partner Agreement" means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)~~

~~(t)~~(z) "Treatment" means the HIPAA definition given at 45 C.F.R. §160.103. ~~means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers related to a patient; or the referral of a patient for health care from one health care provider to another.~~

(aa) "Use" means the HIPAA definition given at 45 C.F.R. §160.103.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: California Civil Code§§ 56.05, 56.06; Health and Safety Code §§ 130200, 130201, 130276, 130277, 130278; 45 C.F.R. §§160.103, 164.304, 164.501.

§126030 CALIFORNIA HEALTH INFORMATION EXCHANGE PRACTICES PRINCIPLES

(a) Participants shall adhere to the following principles of fair information practices:

(1) Openness – There should be a general policy of openness among entities that participate in electronic health information exchange about developments, practices, and policies with respect to individual health information.

(2) Individual Health Information Quality – Health information shall be relevant, accurate, complete, and kept up-to-date.

(3) Individual Participation – Individuals or their personal representatives have the right to:

(A) Ascertain the person responsible for individual health information for an entity, obtain confirmation of whether the entity has specific individual health information relating to the individual, and obtain its location.

(B) Receive their individual health information in a reasonable time and manner, at a reasonable charge, and in a format that is generally accessible by individuals.

(C) Challenge the accuracy of their individual health information and, if successful, to have the individual health information corrected, completed, or amended.

(D) Control the access, use, or disclosure of their individual health information, unless

otherwise specified by law or regulation.

(4) Collection Limitation – There shall be limits to the collection of individual health information. Individual health information shall be obtained by lawful and fair means. Where appropriate, it shall be obtained with the knowledge or consent of the individual or their personal representative. The specific purposes for which individual health information is collected shall be specified not later than at the time of collection.

(5) Individual Health Information Limitation – Use and disclosure of individual health information shall be limited to the specified purpose. Certain use and disclosure shall require consent.

(6) Purpose Limitation - Individual health information shall be relevant to the purpose for which it is to be used and, limited to the minimum information necessary for the specified purpose. The subsequent use shall be limited to the specified purpose.

(7) De-Identified Information – De-identified individual health information shall not be re-identified unless specified in law. If de-identified individual health information is re-identified, it shall be subject to these principles. De-identified individual health information shall not be disclosed if there is a reasonable basis to believe that the information can be used to identify an individual.

(8) Security Safeguards – Individual health information should be protected by appropriate security safeguards against such risks as loss or destruction, unauthorized access, use, modification or disclosure of data.

(9) Accountability – An entity shall comply with laws, regulations, standards and organizational policies for the protection, retention and destruction of individual health information. Any person who has access to individual health information shall comply with those provisions.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126040 TRANSPARENCY AND COMPLAINT PROCESS

(a) Prior to the approval of any demonstration project, the Applicant must provide CalOHII with copies of:
  (1) The Applicant's Notice of Privacy Practices created pursuant to 45 C.F.R. §164.520.
  (2) ~~All of t~~ The Applicant's ~~Data Use Agreement(s)~~ Participants Agreement and a list of the entities included in the ~~data use~~ agreement.
  (3) A description of the Applicant's complaint mechanism required by §126040(d), including any documentation or patient educational materials related to the complaint process.

(b) Once a demonstration project is approved, but prior to the start of the demonstration project, within a specified time frame negotiated with and approved by CalOHII, the Participant must provide:

~~(3)~~(1)A list of all of the Participant's current business associates ~~and trading partners~~ with electronic access to the individual health information disclosed through the demonstration project, with their contact information and a general description of the service(s) provided, including the data shared, the purpose, and whether further dissemination of the data is allowed, regardless of whether the information is de-identified. ~~This requirement may be modified to reflect only those business associates and trading partners with access to the individual health information exchanged through the demonstration project.~~

(A) If a new business associate ~~or trading partner~~ is added after the start of the project, or a business associate agreement ~~or trading partner agreement~~ is modified, the Participant must provide CalOHII with an updated list quarterly ~~within 20 business days of the commencement of the business associate agreement or data exchange partner agreement or the provision of services, whichever is earlier.~~

(B) In CalOHII's discretion, CalOHII may require copies of the Participant's business associate agreements ~~and trading partner agreements~~ be provided to CalOHII. The Participant shall provide copies within five working days from the receipt of written request from CalOHII.

(2)A copy of the EHR Vendor agreement for each Participant.

(c) All unauthorized electronic disclosures or access of individual health information shall be reported to CalOHII within ~~five~~ thirty (30) business days of the detection of the unauthorized access or disclosure. Good faith acquisition of IHI by an employee or agent within the course of coordinating care or delivering treatment services, provided that IHI is not used or subject to further unauthorized disclosure do not need to be reported. A report to CalOHII under this provision does not relieve the Participant from any requirement under any local, state, or federal law.

(d) Participants must ensure there is a mechanism to receive and respond to patient complaints.

(1) Complaints associated with the demonstration project shall be reported and forwarded to CalOHII ~~within 20 business days from the date the complaint is made.~~ quarterly and include ~~(2)~~ ~~T~~the Participant's response to any complaint regarding the demonstration project ~~shall be forwarded to CalOHII within ten business days of the response~~.

(2) Complaints reflecting significant risk to patient privacy and confidentiality of individual health information or patient health and safety attributable to the demonstration project shall be reported to CalOHII immediately.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126042 TRADE SECRET DESIGNATION AND PROTECTIONS

(a) All of the information provided to CalOHII by an Applicant or Participant shall be treated as a public record unless such information is designated to be a trade secret or unless the public interest in maintaining the confidentiality of that information clearly outweighs the public interest in disclosure.

(1) Any records, or portion thereof, which the Applicant/Participant wants to protect as a trade secret shall be submitted in a separate sealed envelope clearly marked on the outside as "Trade Secret Material." For purposes of this section, "trade secret" shall have the same meaning as in the Uniform Trade Secrets Act, *Civil Code section 3426* et seq. The Application shall contain a declaration under penalty of perjury describing why the Applicant/Participant believes the material is a trade secret. After review, CalOHII will either grant the trade secret request and keep the material confidential, or deny the request, return all copies of the trade secret material to the Applicant, and not consider the trade secret material in its determination. CalOHII's refusal to grant a requested claim of trade secret does not excuse the Applicant from establishing all elements of the demonstration project application. Any material which CalOHII agrees to consider as a trade secret shall be exempt from disclosure under the Public Records Act, *Government Code section 6250* et seq. Records for which CalOHII has denied protection as a trade secret shall also be exempt from disclosure under the Public Records Act during the time the records are in the possession of CalOHII.

(2) The Applicant/Participant shall have the sole burden of designating, at the time of its submission, any specific information that it believes should be treated as confidential and the reasons therefore.

(b) Requests for Confidentiality. A request for confidential treatment of any information received in connection with any demonstration project application or report submitted to CalOHII must accompany the submission of such information. The confidential information must be submitted separated from the other parts of the filing and marked "Confidential Treatment Requested." The request for confidentiality should not contain confidential information, as requests for confidentiality will be available for public inspection. Confidential Treatment Requests must be signed by the person making the application or report and contain the following:

(1) A statement identifying the information which is the subject of the request, the application or report it relates to, and a reference that the request is made pursuant to this provision.

(2) A statement of the grounds upon which the request is made, including (if applicable) a statement as to its confidentiality and the measures taken to protect its confidentiality, and a statement of the adverse consequences which are expected to result if the information is disclosed through the public records of CalOHII.

(3) A statement of the specific time for which confidential treatment of the information is necessary and the basis for such conclusion.

(4) If appropriate, a statement of the extent to which such information has been previously disclosed or will be disclosed in the future.

(c) Granting of Request. If a request for confidential treatment is granted, the person making such request will be notified in writing, the information will be marked "confidential" and kept separate from the public file, and the application or report will be noted with the following legend: "Additional portions of this filing have been granted confidential treatment pursuant to Section 126042 and are contained in a separate confidential file."

(d) Information contained in confidential files shall only be disclosed to authorized representatives of the Applicant/Participant or other governmental agencies as necessary for them to perform their constitutional or statutory duties or as required by law.

(e) In the event of a receipt of a subpoena request for designated confidential materials, before the disclosure, CalOHII will make a reasonable attempt to notify the submitter of the information before the mandated disclosure, if the notification is not prohibited by law.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Civil Code § 3426; Government Code § 6250 et seq.; California Health and Safety Code §§ 130276, 130277,130278, 130282.

§126050 ~~HEALTH INFORMATION EXCHANGE~~ PERMITTED PURPOSES FOR EXCHANGING HEALTH INFORMATION

(a) Permitted purposes. Individual health information ~~exchanged or accessed~~ disclosed through an HIO or ~~a direct~~ an independent directed exchange shall be limited to:
(1) Treatment.
(2) Reporting to Public Health Officials for immunizations, bio-surveillance and mandated reporting.
(3) Quality reporting for meaningful use to Centers for Medicare and Medicaid Services and the California Department of Health Care Services.
(4) HIPAA mandated transactions consistent with 45 C.F.R . §162.900 through 45 C.F.R. §162.1802 for transaction standards and code sets.

(b) Permitted secondary purposes. Individual health information after it is disclosed through an HIO or independent directed exchange may be used or disclosed for any permitted purpose

allowed by law that is specified in the Participant's Notice of Privacy Practices created in accordance with 45 C.F.R. §164.520.

(c) These provisions do not apply to business practices that use faxes or emails.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279~~.~~ ; 45 C.F.R. §162.923, §164.520.

§12606055 ~~NOTICE AND CONSENT; EXCEPTIONS~~; INFORMING REQUIREMENTS; AFFIRMATIVE CONSENT; REVOCATION OF CONSENT

(a) ~~Notice~~ Informing Requirements

(1) Prior to requesting an individual or the individual's personal representative to consent to permit the electronic exchange of health information among separate, unaffiliated entities, ~~an entity~~ Participant shall provide notice to the individual or the individual's personal representative, which at a minimum shall contain statements describing:

(A) Electronic exchange of health information.

(B) Uses of IHI, which may incorporate the Participant's Notice of Privacy Practices created in accordance with 45 C.F.R. §164.520, if appropriate.~~data exchanged using electronic health information exchange~~

(C) Benefits and risks associated with disclosing IHI through an HIO or independent directed exchange, including the exchange of sensitive health information, such as HIV status, mental health records, reproductive health records, drug and alcohol treatment records, and genetic information which could be inferred or embedded in information that is made available ~~in the exchange~~ through an HIO or independent directed exchange.

(D) Consent requirements. ~~for electronic health information exchange~~

(E) Specific exceptions to the consent requirements for electronic exchange of health information ~~exchange~~ for mandated public health reporting and for transmitting mandated HIPAA transactions and code sets.

(F) Specific exceptions to the consent requirements ~~for electronic health information exchange~~ in emergency situations.

(G) Process for revoking consent, including a contact name, phone number, email address, and website.

(H) When the revocation of consent is effective.

(b) Affirmative Consent

(1) Before an individual's individual health information is electronically ~~exchanged~~ disclosed through an HIO or independent directed exchange, ~~an entity~~ Participant shall obtain written affirmative consent documenting the individual's or the individual's personal representative's choice to electronically ~~exchange~~ disclose the individual's

individual health information or verify the individual's consent in a centralized consent registry.

(2) Obtaining affirmative consent documenting the individual's or the individual's personal representative's choice to electronically exchange their individual health information under this regulation does not necessarily relieve the ~~entity~~ Participant from obtaining other legally required authorizations to disclose health information if other laws impose additional or different requirements that are not satisfied in the consent obtained pursuant to this regulation.

(3)Emergency situations

(A) A Participant may disclose to a ~~licensed health care~~ CMIA provider ~~may access~~ an individuals' ~~individual~~ health information through an HIO or independent directed exchange when:

1. The individual requires emergent care;
2. The individual or the individual's personal representative is incapable of consenting;
3. The individual or the individual's personal representative has not explicitly denied or withdrawn consent on a previous occasion; and
4. It is in the best interest of the individual, as determined by the treating health care provider.

(4) Mandated public health reporting. Affirmative consent is not required for mandated public health reporting disclosures.

(5) Mandated HIPAA transactions and code sets. Affirmative consent is not required for mandated HIPAA transactions and code sets.

(c) Revocation of consent

(1) An individual or the individual's personal representative may revoke their previously granted consent to the electronic exchange of health information among separate, unaffiliated entities by contacting the designated contact person or ~~entity~~ Participant as described in the ~~Notice required~~ informing requirements ~~by~~ in section (a).

(2) After the effective date of the revocation of consent, the ~~demonstration project~~ Participant ~~or health information exchange service Participant~~ shall not allow the individual's ~~individual~~ health information to be ~~electronically exchanged~~ disclosed through an HIO or independent directed exchange unless and until the individual or the individual's personal representative reinstates consent.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126060 REQUESTS TO DEVELOP ALTERNATIVE REQUIREMENTS

(a) An Applicant may request CalOHII to develop an alternative requirement in sections 126050, 126055, 126070, 126072, 126074, and 126076, for the Applicant's demonstration project if the Applicant is currently unable to comply with the requirement or has an alternative policy that it wants to test. All requests to develop alternative requirements must be submitted to CalOHII in writing, and include:

(1) The reason for the request.

(2) All supporting documentation, such as:

(A) If the reason is related to implementation delays, state the timeframe in which the requirement will be implemented.

(B) A description of, and copies of:

(i) Alternate privacy and security provisions that would provide similarly adequate compliance with the California Health Information Exchange Practices Principles,

(ii) Clear delineation of the purpose and the roles of those who may have access to the individual health information and any permitted subsequent use of the information, and

(iii) Information on the governance structure and evaluation of security compliance.

(b) In granting requests to develop alternative requirements, CalOHII will consider, but is not limited to the following factors:

(1) General factors:

(A) The proposal will advance the knowledge and development of privacy and security standards in a new area;

(B) Alternative requirements can provide similar compliance with the principles, without jeopardizing privacy and security of IHI;

(C) Patient safety concerns are significant;

(D) The technology is not readily available; and/or

(E) Insufficient benefit to individual privacy interests as compared to the costs or other legitimate burdens that would be incurred.

(2) Purpose limitations requirements in §126050

(A) The purpose is consistent with State law and not preempted by HIPAA;

(B) The Applicant can demonstrate adequate oversight to ensure no further disclosure or use of IHI unless the secondary use is consistent with the Civil Code sections 56.10, 56.13, 56.30 and more stringent laws; and

(C) If de-identified data is being used or generated, the recipients of the data are known.

(3) Informing and Consent requirements in §126055

(A) For HIO and Independent Directed exchanges of IHI:

(i) The circumstances ensure that patients or their representatives are made aware that IHI is being disclosed, to whom and for what purpose, and whether they have the right to refuse and if they so choose the option to not permit their health information to be disclosed, what are the possible consequences to them;

(ii) The data being disclosed, whether it is particularly sensitive, and whether the disclosure is narrowly tailored to the need for the information;

(iii) The adequacy of the Applicant's risk assessment and mitigation measures, including history of their compliance with the security provisions; and,

(iv) The comparative costs to implement an affirmative consent model.

(B) For independent directed exchanges, in addition to paragraph (A):

(i) The disclosure is made to another CMIA provider;

(ii) The disclosure is by means of a secure transaction;

(iii) The other CMIA provider has a current treating relationship with the patient;

(iv) The disclosure does not contain particularly sensitive health information nor is the information about another individual;

(v) There is oversight and monitoring of the disclosures to ensure that the disclosures are being made to the intended health care providers and are of the intended patient;

(vi) There is no re-purposing or re-directing of the information by the system vendor;

(vii) The disclosing CMIA provider controls and determines the appropriateness and volume of information to be disclosed; and

(viii) Assurances are obtained and verified that the recipient has appropriately implemented security controls.

(4) Security Controls requirements in §126070-126076

(A) Adequacy of the alternative security controls in addressing the particular circumstance;

(B) Whether the proposed security provision is consistent with a mandatory HIPAA provision;

(C) Cost to implement and potential budget cycles of the participants; and,

(D) Types of IHI being disclosed.

(c) CalOHII shall document in writing each grant of a request to demonstrate an alternative requirement within a reasonable time frame and will make the request and a summary of the basis for the decision publicly available.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126070 SECURITY REQUIREMENTS - GENERAL

(a) All Participants must:

~~Scope These security policies shall apply to individual health information in any form whether accessed, licensed, stored, transmitted or maintained. For individual health information that has not been accessed, transmitted, or received on or after the effective date of these policies, these requirements may be waived under Section 126080.~~

~~(b) General Requirements. Participants must do the following:~~

(1) Ensure the confidentiality, integrity, and availability of all electronic IHI the ~~entity~~ Participant creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under California law.

(4) Ensure compliance with these requirements by the ~~entity~~ Participant's workforce and any entity that receives or uses IHI on the Participant's or recipient's behalf.

(b) All Participants and any recipient of IHI received in a demonstration project, who are a HIPAA covered entity or a business associate of a HIPAA covered entity, are required to comply with the HIPAA security standards in Subpart C of Part 164, 45 C.F.R. §164.302 et seq, with respect to the IHI and any risk assessment must include an evaluation of the additional risk incurred by being a Participant in an exchange of health information.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 56.13, 1798.21, 1798.81.5; Health and Safety Code §§ 130200, 130277, 130279; 45 C.F.R. §§ 164.302, 164.306(a)

§126072 SECURITY REQUIREMENTS – ADMINISTRATIVE CONTROLS

~~A demonstration project participant must do the following:~~

~~(a) Information Security (Organization & Responsibility). An entity shall identify the entity's primary security official who is responsible for implementation and compliance to these~~

~~requirements. Such official shall be identified in such a way that anyone who might have a security issue or concern may contact that person.~~

~~(1) Responsibility & Coordination of Information Security Assets. An entity shall account for information security assets and designate the asset owner(s). Appropriate security controls shall be assigned for each class or group of information security assets. Implementation of specific controls may be delegated by the owner as appropriate. The owner remains responsible for the proper protection of the assets in all cases where delegation occurs.~~

~~(2) Information Security Policy Approvals & Management. An entity shall comply with the following:~~

~~(A) In deciding which security measures to use, an entity shall, at a minimum, take into account the following factors:~~

~~(i) The size, complexity, and capabilities of the entity.~~

~~(ii) The entity's technical infrastructure, hardware, and software security capabilities.~~

~~(iii) The costs/benefits of security measures.~~

~~(iv) The probability and criticality of potential risks to individual health information.~~

~~(B) This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this chapter~~

~~(3) Applications Inventory. An entity shall identify all operating, database, and application assets (e.g. application software, system software, development tools) that support the exchange and processing of individual health information and document the importance of these assets. An application inventory shall include all information necessary in order to recover from a disaster or other business interruption, such as, but not limited to, application logging, type of asset, format, location, backup information, license information, and business value~~

~~(4) Isolating Health Care Clearinghouse Functions. If a health care transaction clearinghouse is part of a larger entity, the clearinghouse segment shall protect and isolate individual health information of the clearinghouse from unauthorized access by the larger organization.~~

~~(b) Risk Management Program. An entity shall develop and implement a risk management program that enables the entity to assess and reduce risk to an acceptable level.~~

~~(1) Risk Assessment. An entity shall periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of individual health information held, created, processed, transmitted or received by an entity.~~

(2) Risk Management & Mitigation. An entity shall implement security measures sufficient to reduce risks and vulnerabilities to:

(A) Protect the confidentiality, integrity, and availability of all individual health information the entity creates, receives, maintains, or transmits.

(B) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(C) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under this chapter.

(D) Take steps to ensure compliance with these requirements by its workforce.

(c) Workforce Security Management. With regard to managing sensitive data, an entity shall ensure that all members of its workforce have appropriate access to individual health information and prevent workforce members from obtaining unauthorized access to individual health information.

(1) Workforce Supervision. An entity shall establish a process for authorizing and managing access provisioning and controls for workforce members. An entity shall supervise workforce members. At minimum, an entity shall supervise workforce members by employing the following guiding principles:

(A) Least access privileges necessary

(B) Default to no access

(C) Review and adjust privilege, if needed, upon change of job duties or other changes that impact the need for access

(D) Promptly remove access to individual health information when access is no longer required

(E) Periodic review of workforce access privileges

(2) Workforce Sanctions & Accountability. An entity shall apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the entity.

(3) Permitted Use of Equipment. An entity shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation, including but not limited to, mobile computing devices that can access individual health information.

(d) Compliance Testing, Audit & Monitoring. An entity shall take steps to ensure compliance of their systems with these security requirements. The security of information systems shall be regularly reviewed. Such reviews shall be performed against these provisions:

~~(1) Non-compliance found. If any non-compliance is found as a result of the review, managers shall, at a minimum:~~

~~(A) Determine the causes of the non-compliance~~

~~(B) Remediate issues found to cause non-compliance, or management shall respond indicating why this risk was accepted or not applicable~~

~~(C) Evaluate the effectiveness of the corrective action, post-implementation.~~

~~(D) Perform appropriate breach reporting, as required by HIPAA, California law and contractual requirements.~~

~~(2) Activity Review & Monitoring (Logs). An entity shall regularly review records of activity and monitor information systems that contain IHI. Review information security controls (such as audit logs, access reports, and security incident tracking reports) for indications of control failure or exploitation of information systems. An entity shall take actions to remediate, as appropriate.~~

~~(3) Evaluation of Policy and Technical Compliance. An entity shall perform and document a technical and non-technical evaluation on an iterative basis that demonstrates due diligence and an active evaluation program. Iterative reviews should be performed whenever environmental, operational, or technical changes occur that may introduce security vulnerabilities.~~

~~(e) Security Incident Management Response, & Documentation. An entity shall address security incidents. An entity shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes. An entity shall take measures necessary to determine the scope of the breach and correct offending deficiencies in security controls to prevent a recurrence of the breach of the information system.~~

~~(f) Frequency of Actions. Activities required by this chapter shall be performed at a frequency determined by an entity based on knowledge of activities and/or changes within the organization, or as required by other legal or contractual obligations.~~

(a) Access Controls. A Participant shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems.

(1) Identity Management (Internal). A Participant shall establish policies and procedures to verify the identity of workforce members who will access the Participant's systems. A Participant shall, at a minimum:

(A) Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be

commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations).

(B) Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization.

(C) Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role.

(D) Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

(2) Single Entity Authentication (Non-Federated). A Participant shall authenticate each authorized user's identity prior to providing access to IHI.

(A) A Participant shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to IHI is the one claimed.

(B) A Participant shall authenticate each user to the level of authorized access that complies with the Participant Agreement.

(C) A Participant shall authenticate users attempting to access IHI from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [See NIST SP 800-63 Rev-1]

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.20, 1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. §§ 164.302, 164.306, 164.308,164.310(b)

§126074 SECURITY REQUIREMENTS – CONTINGENCY PLANNING PHYSICAL CONTROLS

~~(a) Contingency Planning. An entity shall document a comprehensive business continuity plan and recovery strategies including elements related to people, processes, environment, incident management, and coordination with emergency response, crisis communications, and individual health information data. Such a plan should include a listing of identified risks and mitigation or acceptance statements for each risk. (See: Section 126072(b) Risk Management Program). Participants implementing operations subject to these requirements are responsible for understanding and being compliant with applicable federal, state and local legislation and regulatory requirements related to business continuity planning.~~

~~(1) Business Impact Analysis. An entity shall document a Business Impact Analysis that identifies any vulnerability and develop strategies for minimizing risk. The Analysis should describe the potential risks specific to the entity and all critical business components. The BIA shall include, but is not limited to:~~

~~(A) Applications & Data Criticality Analysis~~

~~(B) Change Management~~

~~(2) Recovery Strategies. An entity shall document strategies for business recovery from a serious disruptive event. The recovery strategies should define procedures to be followed to achieve a structured and coherent recovery process. The entity shall review any pre-defined procedures in the event of an actual situation arising following a disruptive event and modify these procedures as appropriate. Defined procedures should include, but are not limited to:~~

~~(A) Incident Management~~

~~(B) Emergency Response~~

~~(C) Crisis Communications~~

~~(D) Disaster Recovery Plan, to include:~~

~~(i) Technical Recovery Plans~~

~~(ii) Facilities~~

~~(iii) Business Recovery Plans~~

~~(3) Business Continuity Plan. An entity shall implement a Business Continuity Plan that details procedures and processes for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages, or makes inaccessible, systems that contain individual health information. Consideration should be given to multi-system approach, inter-disciplines, all locations where IHI resides, and all business process boundaries (interface points). The Continuity Plan shall include, but is not limited to:~~

~~(1) Business Impact Analysis (BIA)~~

~~(2) Recovery Strategies~~

~~(3) Testing and Revision of the Continuity Plan~~

~~(4) Testing & Revision of Contingency Plan. An entity shall create and maintain applications/systems to protect the integrity and availability of individual health information. An entity shall periodically test and revise their contingency plan.~~

(a) Mobile Electronic Device Controls. A Participant shall limit and protect the storage of IHI on mobile electronic computing devices and passive storage media. A Participant shall have a policy directing all workforce members, using any non-managed (user-owned) devices or media, to adhere to the user's entity requirements. Storage of IHI on mobile computing devices and passive storage media is prohibited unless the devices or IHI:

(1) Are encrypted where indicated by risk assessment, and

(2) Legacy medical devices may require alternative controls in lieu of standard controls as allowed by device manufacturers, such deviations from standard controls shall be documented.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.21, 1798.81.5; Health and Safety Code §§1280.15, 130200, 130277, 130279; 45 C.F.R. § 164.308(a)(7)

§126076 SECURITY REQUIREMENTS – FACILITY & EQUIPMENT CONTROLS TECHNICAL CONTROLS

~~(a) Facility Access Controls. An entity shall limit physical access to its information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.~~

~~(1) Physical Access Management. An entity shall safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft, including procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. An entity shall document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)~~

~~(2) Communications and Operations Management. An entity shall assign responsibilities for the management and operation of all information processing facilities that handle individual health information. An entity shall establish formal exchange policies, procedures, and controls to protect the exchange of information through the use of all types of communication facilities.~~

~~(b) Device & Media Controls. An entity shall control, administer and maintain a record of the consignment of hardware and electronic media that contain individual health information and any person responsible therefore and maintain the inventory of such assets~~.

~~(1) Mobile Electronic Device Controls. An entity shall limit and protect the storage of individual health information (IHI) on mobile electronic computing devices and passive storage media. An entity shall have a policy directing all workforce members, using any non-managed (user-owned) devices or media, to adhere to the user's entity requirements identified in this chapter. Storage of IHI on mobile computing devices and passive storage media is prohibited unless the devices or IHI:~~

~~(A) Are physically secured in accordance with this Chapter~~

~~(B) Are encrypted where indicated by risk assessment, using minimum encryption standards identified in this Chapter~~

~~(C) Legacy medical devices may require alternative controls in lieu of standard controls as allowed by device manufacturers, such deviations from standard controls shall be documented~~

(2) Workstation & Security Equipment Controls. An entity shall implement physical and/or technical safeguards for all workstations that access individual health information, to restrict access to authorized users.

(3) Unsecured IHI Loss Prevention. An entity shall take reasonable steps to prevent the unauthorized removal or transmission of individual health information, including but not limited to, data leakage, laptop or flash drive loss, etc.

(4) Reuse of Media. An entity shall implement procedures for removal of individual health information from electronic media before the media is made available for re-use.

(5) Disposal of Media. An entity shall utilize a method that best meets the entity's business practices and protects the security of individual health information for final disposition of individual health information, hardware, and/or electronic media on which the individual health information is stored.

(A) The media on which the PHI is stored or recorded shall be destroyed in one of the following ways:

(i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or reconstructed. Redaction is specifically excluded as a means of data destruction.

(ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization.

(c) Technical Controls. An entity shall protect individual health information in information systems as specified in these provisions.

(1) Login Monitoring. An entity shall monitor log-in attempts, reporting discrepancies, and take actions to remediate, as appropriate.

(2) OS & DB Hardening / Patch Management. As appropriate, an entity shall comply with the following for the protection of individual health information:

(A) Apply patches or use other appropriate mechanisms (e.g., update the operating system (OS) and databases) on a timely basis

(B) Harden and configure the OS and databases to address security vulnerabilities

(C) Install and configure necessary security controls

(D) Regularly test the security of the OS and databases to ensure that the previous steps address known security issues

(3) Malicious Code Protection. An entity shall take appropriate steps to protect against malicious software. In addition, an entity shall incorporate a mechanism to detect, mitigate the effect of malicious software, and immediately report malicious software to the primary security official or designee for response if necessary.

(4a) Email & Messaging Security. ~~An entity~~ A Participant shall safeguard electronic mail and messaging containing ~~individually identifiable health information~~ IHI in its possession.

(5b) Audit Controls. ~~An entity~~ A Participant shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ~~individually identifiable health information~~ IHI. The audit log parameters listed below are required for Participants:

- Login ID (successful and unsuccessful attempts)
- Events (create, read, update, delete)
- Timestamp (date, time)
- Role (e.g. doctor, nurse, admin, billing, IT)
- Unauthorized accesses

~~(d) Network Security Management. An entity shall protect the networks and infrastructures that maintain or transmit individual health information.~~

~~(1) Perimeter Controls and Management. An entity shall identify and include, or reference, security features, service levels, and management requirements of all network services in any network services agreement, whether these services are provided in-house or outsourced. Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and a system to detect intrusion.~~

~~(2) Intrusion Detection. An entity shall implement an internal system to detect intrusion attempts. The entity shall document and report successful intrusions to the primary security official or designee for response.~~

(c)(3) Consistent Time. ~~An entity~~ A Participant shall take steps to ensure clocks of all relevant information processing systems within an organization are synchronized using an accurate reference time source using the Network Time Protocol (NTP).

(d) Data Assurance. A Participant shall protect IHI from unauthorized alteration or destruction. A Participant shall implement technical security measures to guard against unauthorized access to, or modification of, IHI that is being transmitted over an electronic communications network.

(1) Encryption & Cryptographic Controls. A Participant shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect IHI. Participants shall utilize the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or its successor, should be periodically reviewed for updated information as part of each Participant's internal best practices.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. § 164.306(a), 164.308(a)(5),164.310, 164.312.

§126078 SECURITY REQUIREMENTS – ACCESS CONTROLS

(a) Access Controls. An entity shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems.

(1) Identity Management (Internal). An entity shall establish policies and procedures to verify the identity of workforce members who will access the entity's systems. An entity shall, at a minimum:

(A) Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations).

(B) Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization.

(C) Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role.

(D) Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

(2) Single Entity Authentication (Non-Federated). An entity shall authenticate each authorized user's identity prior to providing access to individually identifiable health information.

(A) An entity shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to individually identifiable health information is the one claimed.

(B) An entity shall authenticate each user to the level of authorized access that complies with the entity's level of trust agreement with the external exchange entity.

(C) An entity shall authenticate users attempting to access individually identifiable health information from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [See NIST SP 800-63 Rev-1]

(3) Authentication Across Multiple Participants (Federated).

(A) If an entity is participating in a trust network HIE:

(i) The trust network shall manage entity authentication for those participating on the trust network, and

(ii) An entity shall manage user authentication only for those participants participating on the trust network.

(B) If the user authentication process is across multiple systems or entities:

(i) An entity shall implement the agreed upon authentication process among the participants in the trust network.

(C) An entity participating in the trust network shall implement a trust agreement.

(D) The entity shall adopt an authentication solution that incorporates the authorization requirement of this chapter. l.

(4) Authorization & Access Control.

(A) An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with state requirements:

(i) Data Source;

(ii) Entity of Requestor;

(iii) Role of Requestor;

(iv) Use of Data;

(v) Sensitivity of Data;

(vi) Consent Directives of the Data Subject

(B) An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement.

(5) Password Management. Where an entity uses password authentication, it shall require passwords to be created, changed periodically, safeguarded, and of sufficient length and complexity to protect individual health information.

(A) Note: As applicable, passwords shall be used for all mobile computing devices and passive storage media that contain IHI.

(6) Session Controls. An entity shall implement procedures and technical controls to protect against the unauthorized access to individual health information via workstations, which can include, but are not limited to:

(A) Setting session timeout due to inactivity

(B) Password protection for locking screens

(C) Lockout based on unsuccessful logon attempts

(D) Turn on access (security event) logs and regularly review

(E) Limit physical access to workstations

(b) Data Assurance. An entity shall protect individual health information from unauthorized alteration or destruction. An entity shall implement technical security measures to guard against unauthorized access to, or modification of, individual health information that is being transmitted over an electronic communications network.

(1) Encryption & Cryptographic Controls. An entity shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect individually identifiable health information. Participants shall utilize the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or its successor, should be periodically reviewed for updated information as part of each organization internal best practices.

(2) Integrity Controls. An entity shall implement security measures to safeguard electronically transmitted individual health information from being modified without detection until disposed. This includes implementation of electronic mechanisms to corroborate that individual health information has not been altered or destroyed in an unauthorized manner.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. §§ 164.308(a)(4) & (a)(5),164.312

§126080 REQUESTS TO WAIVE REQUIREMENTS

(a) An Applicant may request CalOHII waive a requirement of sections 126050, 126060, 126070, 126072, 126074, 126076, and 126078 for the Applicant's demonstration project if the Applicant is currently unable to comply with the requirement. All requests for waivers must be submitted to CalOHII in writing, and include:

(1) The reason for waiver request

(2) All supporting documentation, such as:

(A) If the reason is related to implementation delays, state the timeframe in which the requirement will be implemented

~~(B) A description of, and copies of alternate privacy and security provisions that would provide similarly adequate compliance with the California Information Exchange Practices Principles.~~

~~(b) Granting waivers of requirements is in the sole discretion of the Director of CalOHII.~~

~~(c) The Director of CalOHII shall document in writing each grant of a waiver of a requirement within a reasonable time frame.~~

~~(1) Unless a waiver is expressly granted in writing, Participants must comply with all requirements of these regulations.~~

~~Authority: California Health and Safety Code §§ 130277, 130278.~~
~~Reference: Health and Safety Code §§ 130200, 130277, 130279.~~

~~§126090 HEALTH INFORMATION EXCHANGE DEMONSTRATION PROJECTS OVERSIGHT~~

(a) During the demonstration project, authorized CalOHII representatives may audit Participants for compliance with these regulations, applicable state and federal law for the protection of individual privacy and the confidentiality of electronic health records with appropriate notice to the Participant ~~at any time~~. An audit may include, but is not limited to inspection of:

(1)Privacy and security policies and procedures

(2) Adequacy of the consent informing process

~~(2)~~(3) Training documentation

~~(3)~~(4) Business associate agreements

~~(4)~~(5) ~~Data exchange partner~~ Participant ~~a~~Agreements

~~(5)~~(6) Operations of the demonstration project, including impact of demonstration of alternative requirements.

(b) The Participant must provide CalOHII with any and all requested documentation pertaining to 126090(a) within 10 business days of the receipt of the request or other time frame negotiated by the parties.

(c) CalOHII may conduct a site visit to observe operations of the demonstration project and compliance with these regulations.

(d) If CalOHII determines a Participant is not in compliance with these regulations, a notice of non-compliance will be issued.

(1) A Participant receiving a notice of non-compliance shall submit a plan of correction to CalOHII within 10 business days of the receipt of the notice of non-compliance.

(A) If CalOHII determines the plan of correction does not adequately address the identified instances of non-compliance, it may reject the plan of correction and

request a Participant to modify the plan of correction and resubmit within 5 business days.

(2) CalOHII may terminate a Participant from remaining in a demonstration project or may terminate a demonstration project in its entirety if:

(A) CalOHII determines a Participant has not adequately addressed identified areas of non-compliance; or

(B) If the Participant has not complied with an accepted plan of correction; or

(C) If the non-compliance with the regulations is so egregious as to imminently threaten the security or privacy of the health information held by the Participant.

(3) In the event of a termination, termination of a Participant or demonstration project shall occur in an orderly fashion balancing patient health and safety with any time constraints in the Participant's Agreements with their HIO or other data sharing arrangements.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Government Code§ 11180 et seq.; Health and Safety Code §§ 130200, 130277, 130279.

Appendix F: Revised Statement of Reasons

Proposed Regulations for Demonstration Projects for the Electronic Exchange of Health Information

UPDATED INFORMATIVE DIGEST

Assembly Bill 278 (Stat. 2010 Ch. 227 (Monning), codified at Health and Safety Code § 130275 et seq.), authorizes the Director of the California Office of Health Information Integrity (CalOHII) to approve demonstration projects for electronic exchange of health information. CalOHII has the general authority to enforce State laws mandating the confidentiality of medical information. These projects will test policies and rules to better inform the State and health care stakeholders while the infrastructure for the electronic exchange of health information is being defined over the next several years. By allowing for various demonstration projects, it will be possible to determine how best to protect privacy in accordance with State and Federal laws while enabling electronic exchange of health information.

Pursuant to California Health and Safety Code § 130277, the Director of CalOHII may adopt regulations applicable to demonstration projects using the health information exchange services developed according to the instant division of law. The Director was granted this authority to ensure that testing potential privacy and security policies occurs within acceptable parameters and the parties involved follow the same basic rules.

In response to comments to the proposed regulations issued March 1, 2011, some of the proposed regulations were modified or deleted and new provisions are being proposed.

SECOND STATEMENT OF REASONS AND RESPONSE TO COMMENTS

California was awarded $38.8 million under the American Recovery and Reinvestment Act (ARRA) for electronic health information exchange development in California. Preserving and enhancing confidence in the individual health information contained in electronic health records (EHRs) and the informational systems that protect and connect them is fundamental in achieving the goals of improving health care safety and efficiency. Demonstration projects are critical to the successful implementation of electronic exchange of health information in California and will fulfill the State's

obligations under the ARRA grant to develop privacy and security rules appropriate for individual health information.

A significant change in these regulations is the distinction between affiliated and unaffiliated entities. We received many comments that wanted the demonstration projects to focus upon exchanges of health information between unaffiliated entities. There are concerns that implementing purpose limitations between affiliated entities would be too disruptive and may not be technologically supported at this point in time. Therefore, consistent with the federal cooperative grant requirements to facilitate exchange between unaffiliated entities, we are narrowing our definitions to reflect this narrowed focus. At this point in time, exchanges between affiliated entities will not be the focus of the demonstration projects; however we will continue to gather information about these types of exchanges to better inform this iterative process.

Another significant change was to modify the term “Direct Exchange” to be “Independent Directed Exchange” to reflect the changes nationally on how the directed exchanges are evolving. We define Independent Directed exchanges to represent the very limited, “conduit” type of exchange. This change correspondingly enlarges the scope of the definition of Health Information Organization (HIO) as both independent directed and HIO facilitated exchanges represent the whole universe of possible exchanges for these demonstration projects.

In the provisions for requesting to develop alternative requirements to these regulations, we specifically called out the different factors for consideration of an opt-out or no consent policy for an independent directed exchange of IHI. The name-change of the “Waiver” provisions to “Requests to Demonstrate Alternative Requirements” (DAR) is to clarify that in these demonstrations projects, opportunity to test other requirements and policies is an option.

Rules for Demonstration Projects and Rules for Individual Health Information

As authorized by AB 278, CalOHII is to establish and administer demonstration projects for the electronic exchange of health information. The demonstration projects are to do all of the following:

(1) Identify barriers to implementing health information exchanges
(2) Test potential security and privacy policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information.
(3) Identify and address differences between state and federal laws regarding privacy of health information.

Additionally, CalOHII is to adopt regulations to ensure that all approved demonstration project participants follow consistent rules and work within those parameters as they are engaged in the electronic exchange of health information. At this time, we are not addressing the differences between state and federal laws and it will be the subject of future regulatory actions.

The initial set of regulations primarily addressed the broad parameters for the demonstration projects. We specifically did not address the privacy rules for the exchange of health information, except in a broad "principles-based" approach to fair information practices which is consistent with the federal framework for privacy and security. We received comments that showed some confusion between the health information exchange practice principles (Principles) and the rules for using individual health information (IHI).

From the comments, it has become clear that we need to address the issues concerning the use and disclosure of individual health information (IHI) and the differences between state and federal laws. CalOHII has worked on the issues surrounding the lack of clarity on the rules that apply to health information for many years. In another regulatory package, CalOHII will be proposing regulations on the use and disclosure of IHI to guide the secondary use of IHI after it has been disclosed through an exchange of health information. By separating the use and disclosure of IHI from the rules guiding the demonstration projects, the purpose of these demonstration projects regulations becomes clearer.

The primary purpose of these regulations is to guide the application process and oversight of the demonstration projects. Section 126080 has been re-titled Requests to Demonstrate Alternative Requirements (DAR) and renumbered to section 126060, adding structure and clarity to the concept of testing under demonstration projects.

I. Section 126010: Applicability

We received comments concerning the timing of the termination of the regulations. In response to comments, a new paragraph has been added to reflect the statutory termination date which will provide additional notice of the durational limits of these demonstration projects. The regulations contained in this chapter are mandatory for entities selected to be demonstration project participants. When the demonstration project ends, the demonstration participants will no longer be a demonstration participant and these regulations will no longer apply to the entity. With the change in terminology to use the term "Participant" instead of entity, the terms of the regulations provide notice of this limitation to regulations.

The proposed regulation specified an effective date; however, because additional regulations are envisioned and would have differing effective dates, this provision is being removed from the revised regulations. Usually, effective dates are identified in the history of each regulations and this provision as originally proposed, is not necessary.

II. Section 126020: Definitions

We received comments suggesting that we use HIPAA terms and that HIPAA was well known and primarily used by the stakeholders. The differences between HIPAA and California law necessitates that we use terms other than HIPAA, because in some instances, California law is more stringent and use of a HIPAA term would permit a broader use of individual health information than is permitted under California law or would not be as protective of IHI.

We received many comments objecting to the modification or deviation from HIPAA and other federal terms, unless it was strictly necessary. Also we received comments concerning omitted terms that are needed to begin the harmonization of the California law with HIPAA.

Upon review of the terms used in the proposed regulations, we made revisions. We agree to use the terms as defined in HIPAA for the following:

- Access
- Business Associate
- De-identified
- Disclosure
- Health Care Provider
- HIPAA covered entity
- Treatment
- Use

In light of public comment and to prevent any future regulatory inconsistency that would require rulemaking to correct, we have revisited our approach of repeating the text of the definition of HIPAA terms and have decided to cross reference the HIPAA citation in our definition of HIPAA terms. We believe most individuals who will be referencing these demonstration project regulations will be familiar with HIPAA and that the failure to repeat relevant HIPAA provisions will not cause confusion.

A difficult term to harmonize is “medical information” under Civil Code section 56.05 with the similar terms of “health information”, “individually identifiable health information (IIHI)” and “protected health information” under HIPAA. We use the term “individual health information” (IHI) because the definitions are irreconcilable. To use any of the existing terms would have allowed a “gap” in coverage of one of the laws and to use one of the common terms with a different definition would cause only further confusion on a very significant and critical element. Therefore, we decided to continue to use the term IHI. However, we have revised the previous definition of IHI that was created in the CalPSAB process to remove an ambiguity that was raised in one of the comments and to align both HIPAA and California law.

In response to comments and to further the harmonization of terms between California law and HIPAA, the proposed definitions have been revised, added or deleted. The changes and modifications to definitions are as follow:

(a) “Access” - Revised

In response to comments this definition was changed to be identical to HIPAA’s definition and as such, references HIPAA.

(b) “Affiliated entity”- Added

This term is being added to distinguish when an exchange of individual health information is to be covered by these regulations and when they are not. In response to comments, these demonstration projects will be focusing upon the exchanges of individual health information between unaffiliated entities. This term is necessary to help draw the distinction and is consistent with the term affiliated covered entity used in HIPAA under 45 C.F.R. §105(b), except that for the purposes of these demonstration projects, the term is not limited to only HIPAA covered entities.

(c)~~(b)~~ “Applicant” - No Revision

No changes were made.

(d) “Authorization” - Added

This term is being added to incorporate the need for each Participant and recipient of IHI to perform a HIPAA preemption when determining the content requirements for an authorization under HIPAA and California law. This provision makes it a requirement that each Participant make their own determination.

(e) ~~(c)~~ "Business Associate" - Revised
We used the HIPAA definition and believe with the law harmonization on the permitted uses and disclosure of IHI, the limitations between HIPAA and California law can be made clearer. Under these proposed regulations, we will rely on each organization to apply the appropriate law, as they determine that law to be, consistent with the preemption provisions under 45 C.F.R. §160.202.

(f) ~~(d)~~ "Business Associate Agreement" - Revised

This term is being modified in response to comments that health plans should not be omitted as an initial start to the law harmonization process. Because of the differences in the definitions of providers under the CMIA and HIPAA and the use of organizations not formally recognized under the CMIA, such as clearinghouses and Organized Health Care Arrangements, during the law harmonization these limitations will be made clearer. Under these proposed regulations, we will rely on each organization to apply the appropriate law, as they determine that law to be, consistent with the preemption provisions under 45 C.F.R. §160.202.

(g) ~~(e)~~ CalOHII – No Revision

No changes were made.

(h) "CMIA Provider" - Added

This term is being added to distinguish HIPAA and CMIA terms for "provider." The CMIA limits the types of entities that can use and disclose medical information and is more restrictive by obligating non-provider entities to obtain an authorization to disclose IHI that was previously created or received or is derived from a CMIA provider or a health care service plan. Such increase of privacy protections under the CMIA makes California law more stringent. The inclusion of this definition is necessary to lay the foundation for the use of IHI after it has been disclosed through an HIO or independent directed exchange of health information. Similar to the treatment of HIPAA terms, we have chosen to not reiterate the provision of the law and are incorporating the term by reference.

(i) ~~(f)~~ "De-identified health information" – Revised

We received one comment objecting to the phrase "deemed adequate" if the information is de-identified in compliance with 45 C.F.R. §164.514. The purpose of this definition is to set a framework on what is meant by the term "de-identified health information." We agree more information on this type of data and the processes defined under HIPAA is

needed. In the transparency requirements under section 126040, we use this term to collect information to start that work. As we are adopting the HIPAA definition, which includes the reference to 45 C.F.R. §164.514, at this point in time we are not ready to make any modifications HIPAA's definition and this can be the subject of further work by stakeholder groups in the future.

~~(g)~~ "Direct Exchange" - Deleted
When we first proposed the term "Direct Exchange," the type of exchange envisioned is now being called an "independent directed exchange" as there are facilitated directed exchanges which involve third parties. The third parties facilitating directed exchanges would come under the definition for HIO and we are deleting the term "direct exchange" and creating below a term of "Independent Directed Exchange."

(j) "Disclosure" - Added

As suggested in a comment, this HIPAA term is being added and used in these proposed regulations. HIPAA's "disclosure" term includes the term "access" as well as release, transfer and divulging of information to an outside entity which best describes the action occurring in an exchange of health information. We are using the term "disclosure" instead of "access" to be consistent with HIPAA's broader use of these terms.

(k) ~~(h)~~ "Electronic Health Record" - Revised

The proposed definition is being modified in response to comments to reflect the definition as used in section 13400 of HITECH. One commenter suggested that the definition of qualified electronic health record, as defined in 45 C.F.R. §170.102, should be used instead. For our purposes, the qualified EHR is too narrow of a definition as it fails to capture the necessary functions beyond what is needed to qualify for enhanced reimbursement under meaningful use.

(l) "EHR Vendor Agreement"- Added

This proposed definition is to facilitate further transparency in these demonstration projects, as described in section 126040. CalOHII will be seeking to obtain copies of the contracts or other arrangements that specify the terms and conditions for the EHR systems. In the CalOHII stakeholder process, we have heard antidotal instances where EHR vendors may be seeking prolonged access or ownership over the individual health information and in these demonstration projects we will be evaluating the EHR vendor's access to IHI and other terms and conditions.

~~(i)~~ "Entity" - Deleted

This term is being deleted in response to comments that said the use of this term may cause confusion.

(m) "Governmental authority" - Added

This term is being added because when we made more specific the term "Participant," we needed to include this term, as it is used in Health and Safety Code section 130276 as a possible Participant in these demonstration projects. In this definition, we specifically call out that public health authorities have specialized units that meet this definition and we want to encourage them to apply to be a demonstration project.

(n) ~~(j)~~ "Health Care Provider" - Revised

In response to comments this definition was changed to be identical to HIPAA's definition and as such, references HIPAA. As previously noted, this term is in contrast to the definition of CMIA Provider.

~~(k)~~ "Health information "- Deleted

This HIPAA term is being deleted as it does not reflect the needed harmonization of the state and federal laws.

~~(n)~~ "Health Information Exchange" (HIE) - Deleted

Due to the number of public comments regarding the confusion of this definition, as well as the lack of clarity in any federal or local definition, we have removed "HIE" from the regulations. All exchange references are to the disclosure of individual health information through an HIO or independent directed exchange.

(o) ~~(m)~~ "Health Information Organization" (HIO) - Revised

This term is being modified in response to comments to clarify that it pertains to an entity separate from the entity that holds and intends to disclose the information. An HIO facilitates the electronic exchange of health information and may have momentary access to the IHI and/or may take on a governance role in overseeing the exchange. For example, the State Designated Entity under Health and Safety Code section 130251, depending on their role in the governance and/or facilitating exchanges, could be an HIO. The key is that this third party has access to the IHI or may be exerting some type of "governance" over the disclosures. At this point in time we are trying to capture the roles of the third parties to the greatest extent possible. Through the

demonstration projects and the stakeholder collaborative processes, more refined distinctions can be made iteratively.

We added the term “unaffiliated” to distinguish from internal EHR utilization and the functionality of an HIO. Also, in these proposed regulations, we are starting with only two types of exchanges: Independent Directed and HIO Facilitated. We deleted the reference to the direct exchanges. The term “Independent Directed Exchange” indicates that the exchange is between the two parties without an intermediary who is providing governance over the exchange and/or who has access to the individual health information. We are using the term “Independent Directed Exchange” to apply to an exchange where the nexus between the two Participants is merely a conduit.

HIOs and Independent Directed Exchanges are complementary, and are intended to collectively include all of the possible exchange scenarios. Within the demonstration projects, the variations in the types of HIO facilitated and governed exchanges will inform the development of best practices and if necessary, additional regulations specific to these differences. At this time, this definition serves to highlight there are differences between Independent Directed Exchange and HIO facilitated exchanges.

(p) “HIPAA” - Added

This term is being added to reflect the common abbreviation of the Health Insurance Portability and Accountability Act of 1996 as amended by subsequent legislation and the implementing Privacy, Security and Enforcement Rules under 45 C.F.R. Part 160 and Subparts A, C, D and E of Part 164.

(q) “HIPAA covered entity” - Added

This term is being added in response to one comment that said that the use of the term “entity” caused confusion. This term is incorporating the HIPAA definition of covered entities and is to help facilitate the harmonization of state and federal requirements.

(r) “Independent Directed Exchange” - Added

This term is being added to replace the definition for “Direct Exchange”. In the time period that these proposed regulations were under development, the term Directed Exchange has evolved into two types of directed exchanges: those in which a third party facilitating the exchange is considered a conduit and therefore has no ability to access the individual health information and those directed exchanges where a third party does have varying degrees of access to the health information. This term pertains to the conduit type of exchange, where the providers can transmit directly to another, unaffiliated entity.

HIOs and Independent Directed Exchanges are complementary, and are intended to collectively include all of the possible exchange scenarios. Within the demonstration projects, the variations in the types of HIO facilitated and governed exchanges will inform the development of best practices and if necessary, additional regulations specific to these differences. At this time, this definition serves to highlight there are differences between Independent Directed Exchange and HIO facilitated exchanges and in the DAR provisions we start to operationalize these distinctions.

(s) ~~(n)~~ "Individual" – No Revisions.

No changes were made.

(t) ~~(o)~~ "Individual Health Information" (IHI) – Revised

As stated previously, this term was modified to better harmonize state and federal laws. The definition of medical information in Civil Code section 56.05(g) includes medical information in a derivative form from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. This is consistent with the treatment of medical information under California law wherein the rules follow the information. Under HIPAA, individually identifiable health information about the past, present, and future is protected. Also, HIPAA protects oral information and not just protected health information in an electronic or physical form. Both laws seek to protect the information if it can be identifiable.

(u) "More Stringent Law" - Added

This term is being proposed to include the functionality of HIPAA preemptions as it is made more specific in 45 C.F.R. §160.202 and the impact of other more stringent laws that specially protect some types of health information, such a 42 C.F.R. Part 2 and Welfare and Institutions Code section 5828. This phrase is being defined to assist in laying the foundation for the use of IHI after it has been disclosed in an electronic exchange of individual health information.

(v) ~~(p)~~ "Participant" - Revised

This term is modified in response to comments that the applicability be made more specific. In the proposed regulation, the frequent use of the term "Entity" was thought to be unnecessarily confusing, when the use of the term Participant added clarity as to the applicability of the rule. The definition of the term Participant was also changed to

identify the types of entities we think will be seeking to be a Participant and it does not include business associates.

(w) “Participants Agreement” - Added

This term is being added to give a name to a type of trust agreement for the exchange of health information that serves to govern the terms and conditions for the disclosure of IHI among unaffiliated, third parties. There are well-known Participants Agreements, such as the DURSA, and in this regulation we are creating a generic term that captures all of these types of agreements.

(x) ~~(q)~~ “Public Health” – Revised

In response to comments, the second sentence concerning consistency with other standards was removed as it was not necessary.

(y) “Sensitive health information” – Added

This is a new definition in response to comments and to lay a foundation for the further work of the demonstration projects. It incorporates the work on the identification of categories of sensitive health by National Committee on Vital and Health Statistics (NCVHS) (Letter to Secretary Sebelius dated November 10, 2010). Also, the definition reflects comments we heard in the work of CalPSAB and NCVHS’s acknowledgement that some sensitivity is patient specific and the health care provider or the health plan, in their interactions with the patient, may become aware of the special needs of the patient.

Defining what sensitive health information is will assist in further discussions on the ability and inability for the electronic health record systems and the HIOs to segregate or shield sensitive health information and to provide additional protective measures, such as enhanced access requirements.

~~(q)~~ & ~~(r)~~ Trading Partner & Trading Partner agreement” - Deleted
These terms are being deleted and the requirement to provide information related to them is also being deleted.

(z) ~~(s)~~ “Treatment” - Revised

In the proposed regulation, we proposed the HIPAA definition, and consistent with the revisions to remove redundant regulatory text, are only providing a reference to the HIPAA citation.

We received one comment that expressed that this term was ambiguous and other comments expressing concern that care management and disease management by health plans were not specifically called out as not being applicable to treatment. At this time we decline to make more specific the law harmonization that is necessary to clarify the incongruences between HIPAA and California law. This is work that needs to be done and during the demonstration projects and in the collaborative stakeholder processes, these matters can be more fully developed. At this point in time, we are using this HIPAA provision is a starting point.

(aa) “Uses” - Added

In response to comments, we are including the HIPAA definition for the term “uses” as this term is often used in conjunction with the term disclosures. This will assist in the harmonization of HIPAA with California law and is necessary to lay the foundation for the use of IHI after it has been disclosed in an electronic exchange of individual health information.

§126030 California Health Information Exchange Practices Principles

In the Initial Statement of Reasons (ISOR), we had stated that these principles of fair information practices would be required, to establish the foundation for trust in the exchange of an individual’s health information. Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information -- their "information practices" -- and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices. Common to all of these are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. In CalPSAB, through a publically vetted process, the principles in section 126030 were created. We are adopting those principles as our fair information practices for the electronic exchange of health information.

We received comments that the principles were not specific enough and were too broad to be complied with. Many commenters took these principles to be the rules for the further use and disclosure of individual health information in lieu of the applicable laws. In future regulatory action, CalOHII will make more specific the applicable rules for use and disclosures, but for the purposes of these demonstration projects, these principles are to guide Participants, in those instances where specific rules do not exist.

Some commenters expressed the opinion that HIPAA has adequately defined the fair information practices needed in the treatment of health information and that the

proposed principles exceeded customary industry practices. The HIPAA Notice of Privacy Practices (NPP) was given as an example of traditional notions of fair information practices. During the CalPSAB development of these principles, HIPAA was often used as the foundation or floor for expectations and the discussions surrounding the NPP practices informed of the need for additional informing related to the electronic exchange of health information and use of HIOs. These principles reflect the benefits derived from HIPAA and also areas where HIPAA created gaps and the community thought more was needed.

One commenter asked how these principles would be enforced. During the demonstration projects we will be looking at the NPP and the actual practices of the Participants to evaluate their practices against these principles. In this process we will learn from and evaluate not only the demonstration projects, but these principles of fair information practices.

§126040 Transparency and Complaint Process

The purpose of this provision was to ensure that CalOHII collects sufficient information from these demonstration projects to:

1. Further develop rules for uses and disclosures of individual health information that is based upon real-world activities and not just what is reported in the stakeholder meetings.
2. Monitor the demonstration projects to ensure that individual health information is being properly safeguarded.

In Health and Safety Code section 130279, CalOHII is charged with establishing and administering demonstration projects that enhance trust of the stakeholders. The lack of transparency has been a long concern of many stakeholders, especially related to the actions by business associates.

We received comments that expressed that the collection of information concerning the Participants' business associates and trading partners was going to be too burdensome. Two commenters proposed that we only limit the collection to the entities with access to the IHI disclosed though the demonstration project. Some proposed that we collect the information on an as needed basis, such as when a problem is raised, or that we use statistical sampling.

In these regulations, we limited the collection of the information to those entities that are being given access to the IHI disclosed though the demonstration project and limited the scope of the collection to only business associates. We understand that there are other permitted business relationships under HIPAA that do not require business associate

agreements and there is sharing of individual health information in these arrangements. At this time, we are focused on business associates and through the demonstration projects and stakeholder processes, we will learn about these other relationships and in the future, focus on them.

We believe that the collection of the information listed in section 126040(b)(1) is necessary to inform the development of privacy rules for these types of secondary uses of IHI. Currently, there is a general lack of transparency and oversight over business associates. With the information gathered, we can gain the needed understanding of this segment of the healthcare delivery system. This information could also identify further technological needs for data segmentation. We rejected the other proposed alternatives because we believe that waiting to collect information on business associates until a problem is identified, would be too late and contradicts our objectives and a sampling process, to be statistically valid, will require much of the information we are seeking. We strongly believe that obtaining information about who is obtaining access to individual health information and for what purpose will be essential to the further development of privacy and security policies and regulations.

We are adding a new requirement based upon some of the anecdotal information regarding the practices of EHR vendors. We are asking that each Participant provide us with their EHR vendor agreement. In the stakeholder process, we were told that some vendors may be seeking “ownership” of the medical information in the EHR and we are concerned about the terms and conditions of some of the EHR systems.

We also received comments concerning the requirement to report all unauthorized disclosures or access. The purpose of this requirement is to effectuate the obligation of CalOHII to oversee the demonstration projects. Some commenters thought the five business days were too short of a period of time and that the detection of the breach as the triggering event should be clearly specified. We also received a comment that stated that innocuous unauthorized disclosures or access occur on a regular basis and that an exception is needed for good faith acquisitions by employees. Further work may need to be done to determine why there are so many unauthorized disclosures and access and whether such patterns are impacting the Participant’s ability to detect unauthorized disclosures or accesses that could possibly cause harm.

In the revised, proposed regulations, we have extended the reporting time to 30 days from detection and included a good faith exception, similar to the provision in Health and Safety Code section 1280.15(a) for licensed facilities. Having similar reporting requirements to CalOHII as the state breach reporting requirements should also lessen the business costs to comply and using the 30 days as it is in HIPAA is appropriate for CalOHII’s role in demonstration project oversight.

One commenter expressed the burden of reporting on complaints associated with the demonstration projects that are already required under existing law. To alleviate the redundancy but to ensure notice is given to CalOHII for monitoring and oversight, the reporting requirement is reduced to quarterly. However, if a significant problem is detected, the Participant will be required to report it immediately to CalOHII.

§126042 Trade Secret Designation and Protections

This is a new provision in response to a comment. One commenter thought some of the records that CalOHII may seek in a demonstration project could be proprietary and the Participant would need assurances that such information could be protected. In response to this comment, we have proposed a new section, 126042 for trade secret designation and protections. Under the Public Records Act (PRA), agencies can withhold production of materials if they are a "trade secret". In this provision, we put the burden on the Applicant/Participant to identify what is a trade secret and to justify why it needs such a designation. If the request is granted, the information would be designated as such and would not be made available in a PRA request. This procedure will enable the Applicants/Participants to control what they want to submit and will enable CalOHII to take actions so that a trade secret is not inadvertently made available to the public.

The specific criteria are similar to regulations enacted by other state agencies and are reflective of the criteria to evaluation of trade secrets under Civil Code section 3426 et seq.

§126050 Permitted Purposes for Exchanging Health Information

The purpose of this provision is to regulate the scope of demonstration projects that are going to be tested. With the lack of transparency and the developing technology to support privacy and security, we followed earlier recommendations by CalPSAB to focus on treatment and public health reporting. The concern is that there are powerful economic incentives for patient data and once individual health information is digitalized, its disclosure to others could be unbounded.

We received comments expressing the need for an expansion of the list of permitted purposes for the exchange of health information, including patient access to their medical information and public health. We acknowledge that the list is narrower than all of the other permitted uses and disclosures allowed under law. This was purposeful so that we focused on the most urgent needs, which are:

- The need for treatment that was identified in CalPSAB; and
- To meet the Meaningful Use standards as identified by CMS.

In the revised, proposed regulations, we have added another purpose, to permit the HIPAA mandated transactions as contained in 45 C.F.R. §162.900 through 45 C.F.R. §162.1802. These transaction standards and code sets are required of all covered entities and we believe most entities who are engaged in electronic exchange of health information will be covered entities under HIPAA. The inclusion of these capacities in functionality will assist in the cost effectiveness of the developing administrative functions of EHRs and HIOs. We also propose that these HIPAA mandated transactions be exempt from patient consent, although the subject should be addressed in the informing of patients.

Under section 126060, the process to request to demonstrate alternative requirements (DAR) will permit other demonstration projects to test and demonstrate other purposes and the DAR process itself is a means to assist us in expanding the permitted purposes over time and with better transparency of those purposes.

We also received questions on the rules that apply to health information after it is disclosed through an electronic exchange of individual health information. In the revised regulations, we are adding subdivision (b) which states:

> (b) Permitted secondary purposes. Individual health information after it is disclosed through an HIO or independent directed exchange may be used or disclosed for any permitted purpose allowed by law that is specified in the Participant's Notice of Privacy Practices created in accordance with 45 C.F.R §164.520.

This provision is included to clarify the separation of what information can flow through an HIO or independent directed exchange of individual health information and how the information will be used or further disclosed in the normal business practices of the participants.

We received a comment asking about the application of these regulations to business associates. These regulations will operate similar to existing law. For example, under the CMIA, the use and disclosure of medical information is restricted to the entities identified under law and for specifically delineated purposes. The concept of a business associate is not expressed in the CMIA as it is in HIPAA and any further use or disclosure by a business associate must be performed under the expressed delegation of authority of a CMIA provider of health care as defined in Civil Code section 56.05 (CMIA provider) or health care service plan to maintain compliance with the CMIA. As health care service plans and CMIA providers utilize business associates in the demonstration projects and in the further use and disclosure of individual health

information, we expect the Participants to ensure their business associates are in compliance with both state and federal laws.

We received a comment that expressed that "treatment" should be made more specific to specify that it is for current treatment needs. We decline to make that change as we believe that the term treatment, as defined in HIPAA makes it clear to apply only for current treatment needs as any other use would most likely be healthcare operations.

In response to comments, and in conjunction with the deletion of the definition of HIE, we are expressly stating the provisions limiting permitted purposes for the electronic exchange of individual health information do not apply to business transactions such as faxes or emails. At this time, the demonstration projects are not focused on these limited business practices. The purpose of these demonstration projects are to provide oversight when the business practices are enabled by information systems that link into the health and medical records systems and facilitate the collection of the individual health information to be disclosed. It is these automated functionalities that need further review and are to be included for the purpose of these demonstration projects.

§126055 Informing and Consent; exceptions

This provision is being re-numbered so that a future section 126080 for law harmonization can be added and the term "notice" is being changed to "informing" to foster a differentiation from the "notice of privacy practices" (NPP) and the informing that is necessary with the electronic exchange of health information.

This provision, and the provision that would permit the demonstration of an alternative consent policy that did not require an opt-in consent (formerly known as the waiver provision), were the subject of almost every letter we received. Some commenters said that requiring consent would in and of itself be an insurmountable barrier to the development of exchanges of health information in California. In these comments and in the CalPSAB process we heard for exchanges to become sustainable, a critical mass of IHI must exist in the exchange and requiring consent will not garner enough patients to meet this needed critical mass. One person alluded to this being a public need that over-road the individual's need for privacy of their medical information.

Others thought consent was a necessary threshold, that health information exchanges are in their infancy and unable to handle segregation of sensitive information, that consent is the best approach for California because of the undue risk to privacy and patient trust in the current situation of untested organizational practices, untested technological safeguards, concentration of patient data, expansion of health data accessibility and unclear legal rules.

Some supported the need for consent with surveys and others supported the need to go without consent with other surveys. When this issue was before CalPSAB, we received responses from 33 organizations and 1,232 California residents, solicited by the American Civil Liberties Union. The organizations were split and the individuals wanted an opt-in policy. While implementation issues remained, consensus was reached at CalPSAB in the fall of 2010 for an opt-in policy which was relayed to the Secretary of the California Health and Human Services Agency in January 2011.

In the comments, many asserted that HIPAA was adequate and provides sufficient protections. Another stated that we shouldn't assume that existing law adequately protects patient privacy. In California, we have as the foundation for preserving the confidentiality of individual health information the Confidentiality of Medical Information Act (Civil Code section 56 et seq.) and the Insurance Information and Privacy Protection Act (Insurance Code section 791 et seq.). Also, there are various laws that apply to specific situations and general privacy laws such as the Information Privacy Act (Civil Code section and1798 et seq.) and the state constitutional right of privacy (Cal. Const. Article 1, section 13). Due to the potential preemption of state law by HIPAA and the fact that it is done entity by entity, in California there is no one "rule" for the use and disclosure of health information and a lack of consensus on what the rules are.

One commenter stated that relying solely on consent was ineffective in protecting privacy and that instead there needs to be a comprehensive policy framework that sets clear parameters for access, use and disclosure of personal health information for all entities engaged in e-health and that is vigorously enforced. Another said we should wait until a blue-ribbon panel can advise the state on the best-of the breed model for data exchange or until the weaknesses of each project can be fully assessed and specific remedies are required before each project can go live.

This absence of a comprehensive rule is one of the many factors that went into the decision to require consent. Through continued work of the demonstration projects, transparency of the uses of individual health information, and the CalOHII committees and task groups, a comprehensive set of rules may be developed, but for now there is no comprehensive policy. Without a comprehensive policy on how individual health information can be used or disclosed, and in consideration of the other "risks", a consent requirement puts the patient in a position to weigh the risks and make a decision that is best for them on how their individual health information can be shared.

Many factors were considered as the basis for requiring consent and many of these factors are heavily dependent upon the variations in business practices and the type of electronic record system deployed. These factors are:

- Recognition that digitized health information will be easier to disseminate and when it is disclosed to another record system, it will exponentially expose individual health information to risk of unauthorized use and disclosures.
- For some California populations, consent is required by law. To foster development of consent mechanisms, consent as the starting point makes sense and would be cost effective to have this population incorporated seamlessly into the business systems and processes. Segregating this population out for special handling was disfavored and potentially stigmatizing.
- Notice of the potential uses and future further disclosures will not be guided by a comprehensive set of rules followed by all of the Participants and the potential is very great for variations among Participants.
- Technology to segregate the data and to use more granular access controls are not widely available or used, therefore some types of sensitive health information specifically protected by law may be inadvertently disclosed.
- There are concerns that some electronic health records systems are being used for health care operations and the systems can not comply with minimum necessary requirements in HIPAA.
- There are concerns that many HIPAA covered entities may not be following HIPAA security requirements and there are questions whether existing security controls are actually working and whether entities understand their risk assessments and have an approach to identify and resolve deficiencies in their security programs.
- Innocuous unauthorized disclosures occur on a regular basis.
- No technology being implemented today can prevent a “rogue” workforce member or business associate from doing harm while utilizing their role based access.
- Costs to monitor are high and a large portion of the breaches reported were found because the victim complained and not by the detection capabilities of the electronic health record system.

The current practices for collecting, using and sharing IHI are based on trust. The use of this evolving technological capacity to safeguard confidentiality at the same time facilitate the sharing of vast amounts of health information can place that foundation at risk. There is risk to the patient and there is risk to the provider community. Consent is a mechanism to communicate and set expectations in these evolving times. To foster the further development of exchanges, we cannot wait until there are comprehensive policies and mature technologies. The only feasible option to facilitate continued growth of the electronic exchange of individual health information is consent.

One commenter suggested that there be a hybrid, no consent for treatment and payment and consent for the other uses. Through the life of these demonstration

projects, maybe we will get to a stage where there is a clear and non-controversial comprehensive policy for the use and disclosure of individual health information for treatment and payment, and that consent may not be needed for some types of disclosures. However, collecting consent for the other uses will incur many of the same burdens that stakeholders are objecting to in these regulations and were objected to when CalPSAB initially proposed a hybrid consent policy.

Also, these proposed regulations reflect the fact that one "consent policy" may not fit all types of exchanges and in recognition of that fact, the DAR provisions were included to permit flexibility, transparency and accountability. Some commenters wanted directed exchanges to be exempt from the consent requirements and others were equally emphatic that no exchange of health information should be exempt. At this time in the development of exchanges of health information, the DAR provides a transparent process where the unique circumstances of the exchange of health information can be evaluated was chosen as the most prudent approach to balance the very divergent views of California stakeholders.

(a) Informing

We received comments stating that the proposed elements of the informing were not robust enough to ensure that it is meaningful. Others said that it was too complex and that the HIPAA Notice of Privacy Practices (NPP) should suffice. Part of the purpose of the demonstration projects is to implement an informing and consent process and evaluate the sufficiency of the information provided to the patient. The informing and consent provision is a starting point and will evolve over time as we learn more from the demonstration projects.

Some commenters suggested that the HIPAA NPP is adequate. The historical objection to the NPP is that it really doesn't provide the reader with sufficient detailed information to understand what the implications are to them. A separate informing document is being required for consent to ensure that the risks and benefits of participation are made available to the patient.

To reflect the change in permitted purposes under section 126050(a)(4) for HIPAA mandated transactions and code sets, both the informing requirements under (a)(1)(e) and affirmative consent (b)(5) were changed. The informing document should provide the patient information that these uses and disclosures of their individual health information may occur, and that the patient is not being given the opportunity to consent to these uses and disclosures. The transactions and code sets are required by law for covered entities to comply with and the data elements have very limited variability and are situation specific. There is very little concern that the disclosure will be overbroad and unnecessary and the secondary use of the information is relatively static, as the

information is already in an electronic format and the use of an exchange is not likely to accelerate the secondary use of the information.

(b) Affirmative consent

We received comments concerning the operational problems and burdens in obtaining consent at each interaction and we clarified in the regulations, consistent with previous CalPSAB recommendations, that if a consent registry were available it could be used to alleviate the burden on the provider. The parameters of consent registries will need further policy development, due to the impact on some of California's population for whom "blanket" consent is not legally possible.

We received comments suggesting language changes to clarify the difference in requirements for consent under the regulations versus authorizations required by law and we made these changes.

We received comments that patient safety issues are raised when a patient refuses access to their health information in an emergency situation. We believe that anytime a patient chooses to not permit electronic exchanges of his/her health information, even in an emergency situation, the patient should be counseled about the potential serious impacts on their health and wellbeing and that the counseling be well documented. Because individual health information, once obtained, becomes part of the records of the next entity, the patient is in the best position to make the informed decision and that decision should be respected, similar to an advance directive.

(c) Revocation of consent

We received comments that this provision needs to be clearer, that the request should be in writing, and that a process should be developed if the patient wants to re-instate their previous consent. We purposefully left the process of the revocation open for the demonstration projects to develop the appropriate mechanisms. This is an area where technological capability and policy must develop.

We also received comments asking for clarification on the "prospective" effect of a revocation. The language of the regulation only speaks to the further dissemination of the information after the revocation's effective date. In the notice that informs the patient, it is required that the effective time period for a revocation be provided and it is anticipated that the prospective impact and technological limitations on previously sent information will be explained in the notice. Again, part of the demonstration projects is to develop and test various ways in implementing consent.

We also received comments that a new provision should be added to clarify what happens to the individual health information after the termination of the demonstration project. Because the information is being disclosed for treatment purposes, it will become part of the legal record of the healthcare provider, so the information will remain in the records of the treating providers. If the scope of permitted purposes for exchanges of individual health information expands, a new provision may need to be developed to address what happens to the IHI for those other purposes; however, at this point in time we decline to do so. During the demonstration projects and in the collaborative processes, these matters can be more fully developed.

One commenter also asked for more notice and service to patients who are victims of identity theft. This is not addressed at this time in the development of these regulations and could be the subject of a demonstration project. Also, during the demonstration projects and in the collaborative processes, these matters can be more fully developed.

§126060 Requests to Demonstrate Alternative Requirements

In the Initial Statement of Reasons, the need for the previously-entitled "waiver provision" (section 126080) was twofold: to assist in developing privacy and security requirements based on real use of the IHI and to permit the use of alternatives to foster further innovation. The "wavier" provision was renamed and moved to section 126060 to reflect its role in the demonstration projects as fostering further development of specific policies and requirements. We included additional language to the first provision to more clearly specify that a request to demonstrate alternative requirements (DAR) can be to support development of other policies not specifically addressed or permitted in the regulations.

As stated in the Initial Statement of Reasons, because the current capacity in California was developed locally and regionally, there is no "universal" model for the electronic exchange of individual health information. Each exchange, whether it is exchanging information through an HIO or integrated delivery system (IDS), is very different from other exchanges. Some permit many different purposes for exchange and others are very restrictive. Some entities exchange only very specific data elements and others provide access to all of the health information contained in their system.

Correspondingly, the risks to the privacy and security of the individual health information are different. The DAR process is intended to weigh the risks and to facilitate mitigation of those risks so that exchange capacity can grow without undue risk to the public welfare. It is essential that we capture the business needs and costs to comply with these rules while ensuring transparency and accountability.

We received many comments objecting to the proposal to permit the waiver of consent. Simply, if the opportunity to consent is not provided to the individual, then there must be some other, objective manner in which to protect the public's interests and trust in the safekeeping of individual health information. Building upon that trust, there may be some exchanges of health information where there is little or no meaningful alternative, such a request to run a laboratory test, and the role of the patient and the limited choices available are not meaningful to warrant making the exchange subject to a consent option.

DAR provisions permit transparency and an objective evaluation of an organization's proposed privacy and security practices. The resulting approved and tested privacy and security practices can then serve as the foundation for best practices for other exchanges. DARs are intended to be an integral part of the iterative process for developing comprehensive privacy and security policies for the electronic exchange of individual health information.

We also received comments requesting that any request that was granted under the waiver provision should be publicly available. In response, we added provisions to make the DARs and a summary of the basis for the decision publicly available. Depending on resources, it is our intent to post these DARs on the CalOHII website along with other information we develop during the demonstration projects. We are trying to achieve two goals—to create a standard platform of rules for the demonstration projects and to test alternative policies for the electronic exchange of health information. By making these DAR decisions transparent and based upon objective evaluations of the circumstances of each demonstration project, we believe we can maintain the patient trust we are ultimately trying to build for the electronic exchange of health information.

We received many comments expressing the need to specify the criteria CalOHII will use for granting requests under this provision. Because there are different policies and potential factors to consider when granting a DAR, the proposed provisions cannot be an exhaustive list of factors.

Many commenters referenced directed exchanges and so in these revised provisions, independent directed exchanges are specifically called out in the consent section(b)(3)(B) to reflect the reduced risk to privacy and security due to the design differences between HIO and independent directed exchanges. Because some directed exchanges are being implemented without a specific notice informing the patient and with no opportunity to opt-in or opt out, some potential evaluation factors are listed consistent with some of the comments that were submitted.

In response to comments mentioned above, the revised regulations add specific criteria similar to the factors originally stated in the Initial Statement of Reasons and we have included some of the criteria suggested in the comments to this section. The DAR factors are broken down into these sections:

- General
- DAR for Permitted Purposes (§126050)
- DAR for Notice Informing and Consent (§126055)
- DAR for Security (§126070-126076)

Through the experience of the demonstration projects, we expect these criteria to evolve like the rest of these regulations.

1. General

It is envisioned that this process would apply to those exchanges of individual health information that have incorporated advanced privacy and security protections into their systems or are so narrow in scope, that with adequate security safeguards, they do not pose a threat to an individual's privacy. Some Participants may be at various stages of implementation. Key foundational elements are:

- Demonstrated compliance with the fair information practices
- Transparency of the purpose for the disclosure of IHI,
- Identification of other entities that may have access and the limitations on their subsequent disclosures.
- Demonstrated compliance with security requirements

2. DAR of section 126050: Permitted Purposes

Although treatment, public health and meeting stage 1 of Meaningful Use were identified as essential purposes for electronic exchange of health information, this proposed regulation reflects the awareness that there are many other purposes permitted under law. To encourage Applicants to demonstrate "best practices" in privacy and security and to bring awareness to these other purposes, DAR for permitted purposes are allowed.

The primary concern is that there is so little known about the secondary uses of IHI, therefore, evaluation will be of the scope of the disclosure of IHI for the proposed uses and to whom, and the applicable security measures and oversight. If CalOHII did not test these uses and instead expanded the permitted purposes of demonstration projects for the electronic exchange of individual health information to all of the purposes

allowed by law, these demonstration projects would pose a substantial risk to the underlying trust. Therefore, a more focused approach was decided and these regulations reflect that decision.

For example, Meaningful Use stage 1 encourages patient access to their health information by electronic means. This is an area that is underdeveloped and would be an appropriate area for a DAR and CalOHII strongly encourages these types of demonstration projects.

Another example is quality assessment and monitoring, a permitted use of individual health information in healthcare operations under HIPAA. Although HIPAA requires that the minimum necessary information be used, there are questions on whether there is adequate compliance with that rule and if electronic health records (EHRs) are being used for healthcare operations and whether EHRs can segregate IHI for those purposes.

When quality assessments can be accomplished automatically through certified electronic health records, the output often can be without any patient specific identifiers. CMS, through Meaningful Use, is encouraging eligible professionals and hospitals to develop their capacity to use these electronic tools that are built within the electronic heath record systems. They will capture the data elements and calculate the results for the applicable clinical quality measures by reporting the results, eventually to CMS/Medi-Cal for all applicable patients. This meaningful use "purpose" is consistent with the Principles as it is limited in scope and secondary transmissions of IHI.

3. DAR for section 126055: Consent

One of the goals of these demonstration projects is to foster clearer expectations for businesses and consumers regarding the types of informational practices for which consent should be provided. Various factors, from the type of data being exchanged, to the Participants' relationship with the patient, and the environment of the exchange, are considered in determining whether an alternative consent policy can be implemented without substantial risk to the trust the patient has in the confidentiality and security of their individual health information. The role of the patient in making a meaningful choice in the use of their confidential information is important. These are areas for further demonstration and discussion in the CalOHII stakeholder process.

Many commenters wanted Direct Exchanges to be exempt from the consent requirement. The design of independent directed exchanges reduces some of the privacy and security concerns and by testing demonstration projects involving independent directed exchanges, we believe further refinement of the applicable polices can be done. The additional criteria proposed for consent reflects the reduced risk to

privacy and security as proposed by some of the commenters. Because there are many variations on the independent directed exchange, and some of the issues driving the requirement of consent cannot be resolved simply in the design of the exchange, we are not prepared to make a blanket decision on a consent policy for independent directed exchanges.
The type of health information being shared in an independent directed exchange and the secondary uses and disclosures of the individual health information are of great concern. While these demonstration projects will not be able to explore all of the potential secondary uses of IHI, their appropriateness and the applicable security measures, the risk that this lack of knowledge poses is going to be a factor in granting a DAR.

4. DAR of Section 126070-126076: Security Controls

Another goal of these demonstration projects is to foster trust among the exchange Participants by setting clearer requirements for the security practices. HIPAA provides a solid foundation for the baseline of security requirements and these proposed regulations increased some of these requirements by making an addressable implementation now a requirement that must be met in a specific manner. Also, some gaps existed in HIPAA and these requirements are being proposed to better manage security.

The areas in security that are subject to a DAR do not include security safeguards that are required by HIPAA. An alternative to an addressable HIPAA safeguard made into a specific requirement by the proposed security regulations can be considered if the alternative has comparable security measures. Similarly other alternatives will be considered for a DAR, so long as it provides similar or improved security.

§126070 Security Requirements

We received many comments that suggested we adhere to the requirements set forth by the HIPAA Security Rule. In light of public comments and to prevent any future regulatory inconsistency that would require rulemaking to correct, we have revisited our approach of repeating the text of the HIPAA security obligations and have decided to incorporate by reference the HIPAA security standards in our security requirements.

There appears to be general agreement that the HIPAA Security Rule represents an adequate baseline for organizational security, although, there are a few subject areas in the HIPAA Security Rule that warrant further guidance. These proposed security regulations were identified through stakeholder engagement and discussions in the

CalOHII Security Steering Team, and include seven security provisions that were either not present in the Security Rule, represented areas in an organization where data breaches are typically more prevalent, or the Security Rule did not include sufficient detail for organizations to implement appropriately. As a result, those seven proposed security regulations have been retained and renumbered in association with administrative, physical and technical control functions. They are:

Administrative Control:

- Formerly 126078 (a)(1) now 126072(a)(1) Identity Management
- Formerly 126078 (a)(2) now 126072(a)(2)Single Entity Authentication

Physical Control:

- Formerly 126076 (b)(1) now 126074(a) Mobile Electronic Device Controls

Technical Control:

- Formerly 126076(c)(4) now 126076(a) Email Messaging & Security
- Formerly 126076 (c)(5) now 126076(b) Audit Controls
- Formerly 126076 (d)(3) now 126076(c) Consistent Time
- Formerly 126078(b)(1) now 126076(d)(1) Encryption & Cryptographics Controls

Administrative Controls

Specifically, we have retained a portion of the proposed regulation on access controls, former 126078(a)(1) is now 126072(a)(1) Identity Management and formerly 126078 (a)(2) is now 126072(a)(2)Single Entity Authentication. The access control methodology, Z-BAC, that had been developed through the CalPSAB process, is being deleted. Z-BAC envisioned a very robust access controls based upon a multitude of factors, such as data source, role of requestor, use of the data, sensitivity of the data and consent directives of the data subject. There was universal approval of this approach; however, these provisions were removed, due to the lack of technological support at this time.

We have retained Identity Management (Internal) because identity management is an area where many security breaches occur if online identities are not properly managed. There are several HIPAA provisions that exist in 45 C.F.R. §§ 164.308, 164.312, and 164.514 and when combined with ISO/IEC's recommendation for user access management and NIST's recommendations per assurance level guidance, the result is a more comprehensive proposed security regulation for the demonstration project participant to securely mange the online identities.

We have also retained Single Entity Authentication (Non-Federated) because the current health information exchange landscape requires a more secure authentication process that combines assignment of unique identities, authenticating to the appropriate level of authorized access and requiring two-factor authentication from unsecured locations and devices. Additionally, ONC recently recommended two-factor authentication in a presentation dated 4/13/11. See link for the presentation: http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_12811_954362_0_0_18/hitpc-pstt-recommendations-04-13-11.pdf

Physical Controls

Specifically, we have revised 126076(b)(1) now 126074(a) Mobile Electronic Device Controls to apply to Participants, not entities. HIPAA does not adequately address the current landscape of the ever-changing variation of mobile devices and the accompanying technology with which these devices can quickly upload or download massive amounts of data and are easily lost or stolen. This exposes patients/consumers to security breaches of their health information and endangers the public's trust.

One commenter was concerned that we were permitting devices that are using less than the state of the art in security protections. The purpose of the provision in (a)(2) was to highlight that in those circumstances were legacy devices are no longer supported by the manufacturer, that it is the responsibility of the Participant to ensure that alternative controls are used and well documented.

Technical Controls

Specifically, we have retained formerly 126076(c)(4) now 126076(a) on Email Messaging & Security. We received no comments on this section and believe this section is necessary to help ensure secure transmissions of individual health information.

We have retained and revised former 126076(c)(5), now 126076(b) Audit Controls because audit logs may not be common practice particularly with small practices and, when used, may not be reviewed frequently enough to reliably determine inappropriate access. We added specific criteria on what should be logged, as requested in one of comments. We believe that these data elements represent best practice data elements that were agreed upon by our security stakeholder process. These audit logging parameters will also help to provide a foundation to enable cross entity security event detection and monitoring for the purpose of electronic exchange of individual health information. Another commenters wanted us to ensure that this was a requirement to have functioning. We believe, as phrased, as requiring the implementation of a system

that records the activity, we have sufficiently made clear that participants cannot turn these auditing logs off and it is required of all systems that contain or use individual health information.

We have retained 126076(d)(3) now (c) Consistent Time because this is an essential component for appropriate security monitoring and incident reporting and ensure that audit logging timestamps are consistent not only with a project Participant but also with any business associates of the project Participant. We realize that this is not a requirement under HIPAA, but through the CalPSAB stakeholder process, it was identified as being a necessary security requirement.

We have retained 126078(b)(1) Encryption & Cryptographics Controls because encryption is necessary to the secure exchange of electronic health information. Both state and federal breach reporting laws do not require breach notification if the health information is encrypted. Encryption standards will continue to change so the use of the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source simplifies this process for the providers and ensures that a robust standard is being used to protect IHI. Using NIST standards also ensures compatibility with federal requirements. We received comments not wanting an encryption standard specified. However, based upon the sensitivity of the information, the commonality of the NIST standards and readily availability of products to meet those standards and the stakeholder input on the necessity to keep the encryption stand robust and current, we believe that his standard is appropriate.

§126090 Demonstration Projects Oversight

Oversight is a key element to the demonstration projects and we received some comments regarding the time frame for which a Participant can respond to a request from CalOHII and the potential disruption to the functions if CalOHII were to come unannounced. We agreed to the language change proposed on the need to provide appropriate notice and believe the 10 days is an appropriate benchmark and the parties can negotiate other terms, based upon the scope and urgency of the demand. The proposed regulation is modified to reflect this flexibility.

Other modifications reflect comments as to the scope of CalOHII authority within these demonstration projects. Although the demonstration projects will be testing specific policy areas, the flow of the individual health information is a concern of stakeholders. CalOHII, through the oversight of the demonstration projects, will be assessing the privacy and security of the health information that is made available during the demonstration project and the availability of health information to those who need it.

Also, we received comments concerning termination of demonstration projects in an orderly fashion and in those instances where the problem is one Participant in a demonstration project and not the whole project itself. We made modification to provide this level of flexibility and assurances that patient safety concerns will be the foremost concern in the event of a termination.

Appendix G: Revised Demonstration Project Reference Documentation

HIE Demonstration Project Regulation Documentation References

1. **International Organization for Standardization**
   www.iso.org

2. **National Institute of Standards and Technology**
   http://csrc.nist.gov/publications/PubsSPs.html

3. *NIST Cryptographic Module Validation Program (CMVP)*
   http://csrc.nist.gov/groups/STM/cmvp/index.html

Appendix H: Demonstration Project Metrics Document

What are we testing? Add broad statement about our intent of the survey, including testing of demonstration project regulations. Per AB 278, "It is the intent of the Legislature that the demonstration projects do all of the following:

1. Identify barriers to implementing health information exchanges.
2. Test potential security and privacy policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information.
3. Identify and address differences between state and federal laws regarding privacy of health information.

What do we want the opt-in consent demonstration project to measure and identify?
What questions related to the opt-in consent policy and its implementation to we want to find answers?

Free-form, high level text questions:

1. Is Opt In an administrative burden? How, why, please provide data.
2. What is the cost of Opt In?
3. What is the best way to educate patients on HIE and their information?
4. Can small providers manage an Opt In?
5. Do patients' want the right to affirmatively Opt In or Out?
6. Are patients being clearly informed?
7. Do patients want 'break the glass'?
8. Do patients want segregation of sensitive data?
9. Do patients have any issues with use of their de-identified data?
10. Point of care consent – are patients comfortable with opting in with single consent for information from this particular visit?

11. Prospective consent – are patients comfortable with opting in for today and for future care that has not yet occurred?
12. What is the patients' interest in expressing control over their personal health information in terms of granularity?
13. What is the organization capable of allowing the patients to express high degree of granularity in their opt-in/opt-out?
14. Does your organization use or plan to use a prospective opt-in/opt-out process, or alternatively use a one-time point of care opt- in/opt-out process?
15. Does the patient want one time authorization or prospective consent? From this point forward, or anything in the past and going forward?
16. Time range – patient's decision for consent – how long is consent given- both in history and in future?
17. Break the glass – is it appropriate for someone to opt-out, especially in life-threatening event, religious preferences, cultural preferences, or any other issues related to this topic (ED task group previous work- what was that task group's conclusion—no conclusive recommendation from the task group)?
18. What are the provider rights to viewing the patient's record for their own protection? Ex. Blood-borne pathogen.
19. Note that this document, and the associated documents such as the informing materials, whitepaper, and consent form, would be produced in a manner that is compliant with CA state law and federal in terms of language, accessibility, etc.
20. Need to issue guidance on which questions apply to which populations (those patients that were informed, or not)?
21. It's becoming apparent to this group that we need to structure this process so that it accommodates multiple patient informing and consent events over time. How do we do this? What are the right questions as a function of the threading of care over time? Does the patient's level of understanding change as a function of time?
22. This survey is being asked of the demonstration project participating organizations only. For those patient-focused questions, the demonstration project participants will be asked to capture this information between the providers and the patients in a manner of their choosing.
23. Need to clearly define the denominator or denominators, such as "all patients seen by the department conducting the demonstration project".

24. The survey methodology should be that the providers or staff are intended to provide the survey to patients at the point of care. For those questions where the patients' perceptions are being asked, then, the methodology is for the provider or staff to ask the patients those questions directly. Need to clearly indicate which questions are for providers for summary impressions, vs. those questions designed to be asked for each patient encounter. Some questions may be more suitable for a "focus group" collection methodology. Need to work with the survey evaluation firm to precisely define this aspect of the survey.

#	Measures/Analysis	Quan/ Qual	Response	Count
1	How many patients total were seen? How many patients were offered the education/informing material? How many patients were seen multiple times during the project duration (only need to have education one time)? If your organization is offering a point in time consent, how many patients were offered the consent multiple times? Need to define "patient" (mental competency, age of patient, majority status (legal age), teenage years-where parents do not need to be present/allowed to be present for certain kinds of discussions)	Quan		
2	How many patients opted in?	Quan		

3	Did the patient express any concerns even though they opted in? How many? Did the patient express an interest in deferring decision or learning more before deciding on consent? Was this decision different as a function of the medical care received--a routine or follow up visit or acute illness (was the patient in a situation where they were in a stressful situation where they could/could not make decision)? Was the patient actively engaged in the process (Did the patient have questions, was there conversation)?	Qual/ Quan		
4	How many patients opted out? What was their reason for doing so? Advice to person responding: was patient not engaged, available to make decision at this time due to stress, patient wasn't aware of the process (see questions at end of the list)	Quan/ Qual		
5	Did any return patients change their mind on their subsequent visit to opt in? How many? What was their reason?	Quan/ Qual		
6	Did any return patients change their mind on their subsequent visit to opt out? How many? What was their reason?	Quan/ Qual		
7	Do patients want the choice to opt in? Would patients rather have information available to the doctor without having to consent? How many? (Do we want to revise this question so that it captures the impact to the intersection of the need for information and the quality of care being provided? (overarching question)).	Quan/ Qual		
8	Do patients find the consent form confusing? How many? What was the reason or reasons? For those cases where the patient found the form confusing, was the confusion able to be resolved? If the confusion was resolved, how? What was the process, if any, used to resolve the confusion?	Quan/ Qual		

9	What kind of questions did the patient have after being informed? Please list representative questions.	Qual		
10	Do patients understand that their sensitive health information may be part of the exchange due to the inability of some systems to segregate data at this time? Do patients understand the definition of sensitive health information? What are the cultural issues that impact this process? How do we distinguish legally-defined sensitive information vs. other types of sensitive information (such cultural, religious, personal preferences, etc.)? These issues need to be teased apart and validated by us before being placed into a survey.	Qual		
11	Did they elect to not opt-in due to fear that sensitive information would be included?	Qual		
12	If you provided multiple ways of educating the patient (education packet and video)? What were the preferred patient educational approaches? Please list in order as a summary of all patients that participated in the education process. Should the patient's educational preferences be provided in multiple formats to accommodate differences in patient preferences as a function of factors such as race, religion, gender, etc.?	Qual		
13	From the patients' perspective SHOULD a provider have access to all health information? From the patients' perspective, does a provider NEED to have access to all health information? Would a patient summary document suffice (with the patient's most recent active problems, meds, allergies, etc.)? From a PROVIDER's perspective, what information SHOULD or do they NEED to have available at the point of care? Is there a time range limitation on the applicable data? <break into two question groups: one for the patient perceptions, and one for the provider practice.>	Quan/ Qual		

14	Do patients want their information segregated? (How many patients?) If so, what categories would a patient like to see separated from the remainder of the medical record?	Quan/ Qual		
15	• Mental health/Psychotherapy notes (How many patients?)			
16	• Substance abuse (How many patients?)			
17	• HIV (How many patients?)			
18	• Genetic information (How many patients?)			
19	• Reproductive health (How many patients?)			
20	• Other – Explain (How many patients?)			
21	What portions of their medical records would they like to exercise control over? What type of control would patients like over various aspects of their medical records? How would the patient like to exercise control over their record (such as a web site, or paper forms, or a patient portal, or other mechanisms such as a provider acting as the proxy for the patient)?	Quan/ Qual		
22	Do patients understand that restricting provider's access to any types of information may result in the patient being put at risk by omitting pertinent information from the doctor's review? Are patients willing to take this risk? Does the patient's decision-making ability change this issue (comatose vs. alert)? How would patients like to resolve this issue? How would providers like to resolve this issue?	Quan/ Qual		
23	Are patients willing to share their data with other organizations if it is de-identified (need to ensure patients understand de-identification)? How many? What are the patients' concerns and issues related to the secondary use of their data?	Quan/ Qual		

24	In an emergency case scenario, would the patient like the doctor to have access to all of his/her records? How many? Or, would they maintain that certain records should not be viewed as decided by the patient? How many? Would the patient like to restrict access to certain health data under any circumstances even if their live depended on it (such as for religious preferences)?	Quan/ Qual		
25	How long (minutes) did the consent process take with the patient? What was the average? Longest? Shortest?	Quan		
26	Did another process suffer in that it could not be done or was not done as efficiently as before due to the consent process?	Qual		
27	What is providers' estimate of the cost of the consent process? (include materials, time in educating, etc…)	Quan		
28	Did providers believe the process was manageable? If not, how many? What was the reason?	Quan/ Qual		
29	Did the patients find the informing document helpful? Why?	Quan/ Qual		
30	Did the patients find the informing document confusing? Why?	Quan/ Qual		
31	Had the patients seen any educational material (brochures, video clips, public announcements, DVDs, etc…) on the electronic exchange of health information and patient privacy rights prior to receiving the informing document and the consent form? • How many patients had any exposure to educational material? • What kind of material did they use/see/receive? • Was the material helpful to the patient in making an informed decision in giving/withholding consent? • How many patients had no exposure to any educational material?	Quan/ Qual		

32	Were the patient consent options “meaningful” to them? What can be done to improve the meaningful nature of the consent process from the perspective of the patient?	Qual		
33	What can be done to improve the meaningful nature of the consent process from the perspective of the healthcare provider?	Qual		
34	For those patients that were informed about the consent process, did those patients feel that they were sufficiently educated about the process? Did they feel comfortable making a decision? (Place this question carefully so that it doesn’t introduce survey methodology bias). (These questions should be designed so that no bias is introduced via the questions themselves).	Quan/ Qual		
35	For those patients that didn’t make a decision at the first patient and informing discussion, and for those patients that did not make a decision at that point, why did they not elect to make a decision?	Quan		
36	Outside of this process, what is the patient doing, if anything, to educate themself about the consent process? Has any misinformation been identified (such as an incurred blogger that had broad influence)?	Qual		

Appendix I: California Law: Confidentiality and Disclosure Chart

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
42 CFR § 2.2 Statutory authority for confidentiality of alcohol abuse patient records.	**Alcohol & Drug** **Confidentiality, authorization, and disclosure of alcohol and drug patient records**	§ 2.2 Statutory authority for confidentiality of alcohol abuse patient records. The restrictions of these regulations upon the disclosure and use of alcohol abuse patient records were initially authorized by section 333 of the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970 (42 U.S.C. 4582). The section as amended was transferred by Pub. L. 98–24 to section 523 of the Public Health Service Act which is codified at 42 U.S.C. 290dd–3. The amended statutory authority is set forth below: §290dd–3. Confidentiality of patient records (a) Disclosure authorization Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any program or activity relating to alcoholism or alcohol abuse education, training, treatment, rehabilitation, or research, which is conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except as provided in subsection (e) of this section, be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b) of this section. (b) Purposes and circumstances of disclosure affecting consenting patient and patient regardless of consent (1) The content of any record referred to in subsection (a) of this section may be disclosed in accordance with the prior written consent of the patient with respect to whom such record is maintained, but only to such extent, under such circumstances, and for such purposes as may be allowed under regulations prescribed pursuant to subsection (g) of this section. (2) Whether or not the patient, with respect to whom any given record referred to in subsection (a) of this section is maintained, gives his written consent, the content of such record may be disclosed as follows: (A) To medical personnel to the extent necessary to meet a bona fide medical emergency. (B) To qualified personnel for the purpose of conducting scientific research, management audits, financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, any individual patient in any report of such research,		• Consent • Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		audit, or evaluation, or otherwise disclose patient identities in any manner. (C) If authorized by an appropriate order of a court of competent jurisdiction granted after application showing good cause therefore. In assessing good cause the court shall weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services. Upon the granting of such order, the court, in determining the extent to which any disclosure of all or any part of any record is necessary, shall impose appropriate safeguards against unauthorized disclosure. (c) Prohibition against use of record in making criminal charges or investigation of patient Except as authorized by a court order granted under subsection (b)(2)(C) of this section, no record referred to in subsection (a) of this section may be used to initiate or substantiate any criminal charges against a patient or to conduct any investigation of a patient. (d) Continuing prohibition against disclosure irrespective of status as patient The prohibitions of this section continue to apply to records concerning any individual who has been a patient, irrespective of whether or when he ceases to be a patient. (e) Armed Forces and Veterans' Administration; interchange of record of suspected child abuse and neglect to State or local authorities The prohibitions of this section do not apply to any interchange of records— (1) within the Armed Forces or within those components of the Veterans' Administration furnishing health care to veterans, or (2) between such components and the Armed Forces. The prohibitions of this section do not apply to the reporting under State law of incidents of suspected child abuse and neglect to the appropriate State or local authorities. (f) Penalty for first and subsequent offenses Any person who violates any provision of this section or any regulation issued pursuant to this section shall be fined not more than $500 in the case of a first offense, and not more than $5,000 in the case of each subsequent offense. (g) Regulations of Secretary; definitions, safeguards, and procedures, including procedures and criteria for issuance and scope of orders Except as provided in subsection (h) of this section, the Secretary shall prescribe regulations to carry out the purposes of this section. These regulations may contain such definitions, and may provide for such safeguards and procedures, including procedures and criteria for the issuance and scope of orders under subsection(b)(2)(C) of this section, as in the judgment of the Secretary are necessary or proper to effectuate the purposes of this section, to prevent circumvention or evasion thereof, or		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		to facilitate compliance therewith. (Subsection (h) was superseded by section 111(c)(4) of Pub. L. 94–581. The responsibility of the Administrator of Veterans' Affairs to write regulations to provide for confidentiality of alcohol abuse patient records under Title 38 was moved from 42 U.S.C. 4582 to 38 U.S.C. 4134.)		
42 CFR § 2.64 Procedures and criteria for orders authorizing disclosures for noncriminal purposes.	**Alcohol & Drug** Authorizing disclosures for noncriminal, legally sought purposes, including the provision of notice, use in review of evidence, and criteria for obtaining the information.	§ 2.64 Procedures and criteria for orders authorizing disclosures for noncriminal purposes. (a) Application. An order authorizing the disclosure of patient records for purposes other than criminal investigation or prosecution may be applied for by any person having a legally recognized interest in the disclosure which is sought. The application may be filed separately or as part of a pending civil action in which it appears that the patient records are needed to provide evidence. An application must use a fictitious name, such as John Doe, to refer to any patient and may not contain or otherwise disclose any patient identifying information unless the patient is the applicant or has given a written consent (meeting the requirements of these regulations) to disclosure or the court has ordered the record of the proceeding sealed from public scrunity. (b) Notice. The patient and the person holding the records from whom disclosure is sought must be given: (1) Adequate notice in a manner which will not disclose patient identifying information to other persons; and (2) An opportunity to file a written response to the application, or to appear in person, for the limited purpose of providing evidence on the statutory and regulatory criteria for the issuance of the court order. (c) Review of evidence: Conduct of hearing. Any oral argument, review of evidence, or hearing on the application must be held in the judge's chambers or in some manner which ensures that patient identifying information is not disclosed to anyone other than a party to the proceeding, the patient, or the person holding the record, unless the patient requests an open hearing in a manner which meets the written consent requirements of these regulations. The proceeding may include an examination by the judge of the patient records referred to in the application. (d) Criteria for entry of order. An order under this section may be entered only if the court determines that good cause exists. To make this determination the court must find that: (1) Other ways of obtaining the information are not available or would not be effective; and (2) The public interest and need for the disclosure outweigh the potential injury to the patient, the physician-patient relationship and the treatment services.		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		(e) Content of order. An order authorizing a disclosure must: (1) Limit disclosure to those parts of the patient's record which are essential to fulfill the objective of the order; (2) Limit disclosure to those persons whose need for information is the basis for the order; and (3) Include such other measures as are necessary to limit disclosure for the protection of the patient, the physician-patient relationship and the treatment services; for example, sealing from public scrutiny the record of any proceeding for which disclosure of a patient's record has been ordered.		
Health & Safety § 123125. Alcohol and drug abuse records; communicable disease carriers	**Alcohol and drug** Disclosures of Alcohol and drug information	123125. (a) This chapter shall not require a health care provider to permit inspection or provide copies of alcohol and drug abuse records where, or in a manner, prohibited by Section 408 of the federal Drug Abuse Office and Treatment Act of 1972 (Public Law 92-255) or Section 333 of the federal Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970 (Public Law 91-616), or by regulations adopted pursuant to these federal laws. Alcohol and drug abuse records subject to these federal laws shall also be subject to this chapter, to the extent that these federal laws do not prohibit disclosure of the records. All other alcohol and drug abuse records shall be fully subject to this chapter. (b) This chapter shall not require a health care provider to permit inspection or provide copies of records or portions of records where or in a manner prohibited by existing law respecting the confidentiality of information regarding communicable disease carriers.		• Collection, Request, Use, & Disclosure
Evidence Code § 1035.8. Sexual assault counselor privilege	**Sexual assault** Confidential communication between a victim and a sexual assault counselor.	A victim of a sexual assault, whether or not a party, has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between the victim and a sexual assault counselor if the privilege is claimed by any of the following : (a) The holder of the privilege; (b) A person who is authorized to claim the privilege by the holder of the privilege; or (c) The person who was the sexual assault counselor at the time of the confidential communication, but that person may not claim the privilege if there is no holder of the privilege in existence or if he or she is otherwise instructed by a person authorized to permit disclosure.	Evidence Code § 1035.2 Sexual assault counselor" means any of the following: (a) A person who is engaged in any office, hospital, institution, or center commonly known as a rape crisis center, whose primary purpose is the rendering of advice or assistance to victims of sexual assault and who has received a certificate evidencing completion of a training program in the counseling of sexual assault victims issued by a counseling center that meets the criteria for the award of a grant established pursuant to Section 13837 of the Penal Code and who meets one of the following requirements: (1) Is a psychotherapist as defined in	• Collection, Request, Use, & Disclosure • Request Restrictions

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
			Section 1010; has a master' s degree in counseling or a related field; or has one year of counseling experience, at least six months of which is in rape crisis counseling. (2) Has 40 hours of training as described below and is supervised by an individual who qualifies as a counselor under paragraph (1). The training, supervised by a person qualified under paragraph (1), shall include, but not be limited to, the following areas: (A) Law. (B) Medicine. (C) Societal attitudes. (D) Crisis intervention and counseling techniques. (E) Role playing. (F) Referral services. (G) Sexuality. (b) A person who is employed by any organization providing the programs specified in Section 13835.2 of the Penal Code, whether financially compensated or not, for the purpose of counseling and assisting sexual assault victims, and who meets one of the following requirements: (1) Is a psychotherapist as defined in Section 1010; has a master' s degree in counseling or a related field; or has one year of counseling experience, at least six months of which is in rape assault counseling. (2) Has the minimum training for sexual assault counseling required by guidelines established by the employing agency pursuant to subdivision (c) of Section 13835.10 of the Penal Code, and is supervised by an individual who qualifies as a counselor under paragraph (1). The training, supervised by a person qualified under paragraph (1), shall include, but not be limited to, the following	

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
			areas: (A) Law. (B) Victimology. (C) Counseling. (D) Client and system advocacy. (E) Referral services.	
Evidence Code 1010.5. Privileged communication between patient and educational psychologist	**Educational psychologist** Communication between a patient and an educational psychologist.	A communication between a patient and an educational psychologist, licensed under Article 5 (commencing with Section 4986) of Chapter 13 of Division 2 of the Business and Professions Code, shall be privileged to the same extent, and subject to the same limitations, as a communication between a patient and a psychotherapist described in subdivisions (c), (d), and (e) of Section 1010.	Confidential Communications: Evidence Code 992. As used in this article, "confidential communication between patient and physician" means information, including information obtained by an examination of the patient, transmitted between a patient and his physician in the course of that relationship and in confidence by a means which, so far as the patient is aware, discloses the information to no third persons other than those who are present to further the interest of the patient in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the physician is consulted, and includes a diagnosis made and the advice given by the physician in the course of that relationship.	• Collection, Request, Use, & Disclosure
Evidence Code § 1012. Confidential communication between patient and psychotherapist	**Psychotherapy** Communication between patient and psychotherapist.	As used in this article, "confidential communication between patient and psychotherapist" means information, including information obtained by an examination of the patient, transmitted between a patient and his psychotherapist in the course of that relationship and in confidence by a means which, so far as the patient is aware, **discloses the information to no third persons other than those who are present to further the interest of the patient in the consultation, or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the psychotherapist is consulted, and includes a diagnosis made and the advice given by the psychotherapist in the course of that relationship.**	As used in this article, "psychotherapist" means a person who is, or is reasonably believed by the patient to be: (a) A person authorized to practice medicine in any state or nation who devotes, or is reasonably believed by the patient to devote, a substantial portion of his or her time to the practice of psychiatry. (b) A person licensed as a psychologist under Chapter 6.6 (commencing with Section 2900) of Division 2 of the Business and Professions Code. (c) A person licensed as a clinical social worker under Article 4 (commencing with	• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
			Section 4996) of Chapter 14 of Division 2 of the Business and Professions Code, when he or she is engaged in applied psychotherapy of a nonmedical nature. (d) A person who is serving as a school psychologist and holds a credential authorizing that service issued by the state. (e) A person licensed as a marriage and family therapist under Chapter 13 (commencing with Section 4980) of Division 2 of the Business and Professions Code. (f) A person registered as a psychological assistant who is under the supervision of a licensed psychologist or board certified psychiatrist as required by Section 2913 of the Business and Professions Code, or a person registered as a marriage and family therapist intern who is under the supervision of a licensed marriage and family therapist, a licensed clinical social worker, a licensed psychologist, or a licensed physician certified in psychiatry, as specified in Section 4980.44 of the Business and Professions Code. (g) A person registered as an associate clinical social worker who is under the supervision of a licensed clinical social worker, a licensed psychologist, or a board certified psychiatrist as required by Section 4996.20 or 4996.21 of the Business and Professions Code. (h) A person exempt from the Psychology Licensing Law pursuant to subdivision (d) of Section 2909 of the Business and Professions Code who is under the supervision of a licensed psychologist or board certified psychiatrist. (i) A psychological intern as defined in Section 2911 of the Business and Professions Code who is under the supervision of a licensed psychologist or board certified	

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
			psychiatrist. (j) A trainee, as defined in subdivision (c) of Section 4980.03 of the Business and Professions Code, who is fulfilling his or her supervised practicum required by subdivision (b) of Section 4980.40 of the Business and Professions Code and is supervised by a licensed psychologist, board certified psychiatrist, a licensed clinical social worker, or a licensed marriage and family therapist. (k) A person licensed as a registered nurse pursuant to Chapter 6 (commencing with Section 2700) of Division 2 of the Business and Professions Code, who possesses a master's degree in psychiatric-mental health nursing and is listed as a psychiatric-mental health nurse by the Board of Registered Nursing. (l) An advanced practice registered nurse who is certified as a clinical nurse specialist pursuant to Article 9 (commencing with Section 2838) of Chapter 6 of Division 2 of the Business and Professions Code and who participates in expert clinical practice in the specialty of psychiatric-mental health nursing. (m) A person rendering mental health treatment or counseling services as authorized pursuant to Section 6924 of the Family Code.	
Health & Safety § 120705. Confidential reports	**Lab Results STD**	120705. All laboratory reports are confidential, and are not open to public inspection.	120685. Every licensed physician and surgeon or other person engaged in prenatal care of a pregnant woman, or attending the woman at the time of delivery, shall obtain or cause to be obtained a blood specimen of the woman at the time of the first professional visit or within 10 days thereafter. 120690. The blood specimen thus obtained shall be submitted to an approved laboratory	• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
			for a standard laboratory test for syphilis.	
Health & Safety 125105. Confidentiality of test results	**Lab results** Disclosures of lab for prenatal care: determination of rhesus (Rh) blood type	125105. (a) The blood specimen and test results pursuant to subdivision (b) of Section 125085 shall be confidential and shall not be disclosed, except as otherwise provided by law. (b) **No person shall be compelled in any state, county, city, or other local civil, criminal, administrative, legislative, or other proceeding to provide test results determined pursuant to Section 125080 and Section 125085.**	125080. A licensed physician and surgeon or other person engaged in the prenatal care of a pregnant woman or attending the woman at the time of delivery shall obtain or cause to be obtained a blood specimen of the woman. Prior to obtaining the blood specimen, the woman shall be notified of the fact that the blood specimen is going to be obtained. If the blood specimen is not obtained prior to delivery, it shall be obtained at the time of delivery. 125085. (a) As early as possible during prenatal care, a blood specimen obtained pursuant to Section 125080 shall be submitted to a clinical laboratory licensed by the department or to an approved public health laboratory for a determination of rhesus (Rh) blood type and the results shall be reported to both of the following: (1) The physician and surgeon or other person engaged in the prenatal care of the woman or attending the woman at the time of delivery. (2) The woman tested. In addition, as early as possible during prenatal care, a blood specimen obtained pursuant to Section 125080 shall be submitted to a clinical laboratory licensed by the department or to an approved public health laboratory for a test to determine the presence of hepatitis B surface antigen and the human immunodeficiency virus (HIV), and the results shall be reported to both of the following: (A) The physician and surgeon or other person engaged in the prenatal care of the women or attending the woman at the time of delivery who ordered the test, and who shall subsequently inform the woman tested.	• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
			(B) A positive test result shall be reported to the local health officer, with the information required and within the timeframes established by the department, pursuant to Chapter 4 (commencing with Section 2500) of Title 17 of the California Code of Regulations. (2) In the event that other tests to determine hepatitis B infection or HIV infection become available, the department may approve additional tests.	
Health & Safety § 123148. Test results; recording and reporting to patient; Internet or other electronic posting; plain language	**Lab results** Consent by patient for lab results via internet or other electronic means must be consistent with CMIA.	123148. (a) Notwithstanding any other provision of law, a health care professional at whose request a test is performed shall provide or arrange for the provision of the results of a clinical laboratory test to the patient who is the subject of the test if so requested by the patient, in oral or written form. The results shall be conveyed in plain language and in oral or written form, except the results may be conveyed in electronic form if requested by the patient and if deemed most appropriate by the health care professional who requested the test. (b) (1) Consent of the patient to receive his or her laboratory results by Internet posting or other electronic means shall be obtained in a manner consistent with the requirements of Section 56.10 or 56.11 of the Civil Code. In the event that a health care professional arranges for the provision of test results by Internet posting or other electronic manner, the results shall be delivered to a patient in a reasonable time period, but only after the results have been reviewed by the health care professional. Access to clinical laboratory test results shall be restricted by the use of a secure personal identification number when the results are delivered to a patient by Internet posting or other electronic manner. (2) Nothing in paragraph (1) shall prohibit direct communication by Internet posting or the use of other electronic means to convey clinical laboratory test results by a treating health care professional who ordered the test for his or her patient or by a health care professional acting on behalf of, or with the authorization of, the treating health care professional who ordered the test. (c) When a patient requests to receive his or her laboratory test results by Internet posting, the health care professional shall advise the patient of any charges that may be assessed directly to the patient or insurer for the service and that the patient may call the health care professional for a more detailed explanation of the laboratory test results when delivered. (d) The electronic provision of test results under this section shall be in accordance with any applicable federal law governing privacy and security of electronic personal health records. However, any state statute, if enacted, that governs privacy and security of electronic personal health records, shall apply to test results under this		• Consent • Request Alternative Communications

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		section and shall prevail over federal law if federal law permits. (e) The test results to be reported to the patient pursuant to this section shall be recorded in the patient's medical record, and shall be reported to the patient within a reasonable time period after the test results are received at the offices of the health care professional who requested the test. (f) Notwithstanding subdivisions (a) and (b), none of the following clinical laboratory test results and any other related results shall be conveyed to a patient by Internet posting or other electronic means: (1) HIV antibody test. (2) Presence of antigens indicating a hepatitis infection. (3) Abusing the use of drugs. (4) Test results related to routinely processed tissues, including skin biopsies, Pap smear tests, products of conception, and bone marrow aspirations for morphological evaluation, if they reveal a malignancy. (g) Patient identifiable test results and health information that have been provided under this section shall not be used for any commercial purpose without the consent of the patient, obtained in a manner consistent with the requirements of Section 56.11 of the Civil Code. (h) Any third party to whom laboratory test results are disclosed pursuant to this section shall be deemed a provider of administrative services, as that term is used in paragraph (3) of subdivision (c) of Section 56.10 of the Civil Code, and shall be subject to all limitations and penalties applicable to that section. (i) A patient may not be required to pay any cost, or be charged any fee, for electing to receive his or her laboratory results in any manner other than by Internet posting or other electronic form. (j) A patient or his or her physician may revoke any consent provided under this section at any time and without penalty, except to the extent that action has been taken in reliance on that consent.		
Penal Code § 7530.	**Lab test results of prisoners**	7530. The following procedures shall apply to testing conducted under this title: (a) The withdrawal of blood shall be performed in a medically approved manner. Only a physician, registered nurse, licensed vocational nurse, licensed medical technician, or licensed phlebotomist may withdraw blood specimens for the purposes of this title. (b) The chief medical officer, as specified in Chapter 2 (commencing with Section 7510), shall order that the blood specimens be transmitted to a licensed medical laboratory which has been approved by the State Department of Health Services for the conducting of HIV testing, and that tests including all readily available confirmatory tests be conducted thereon for medically accepted indications of exposure to or infection with HIV. The State Department of Health Services shall adopt standards for		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		the approval of medical laboratories for the conducting of HIV testing under this title. The State Department of Health Services shall adopt standards for the conducting of tests under Section 7530. Testing for hepatitis B or C may be conducted by any licensed medical laboratory approved by the chief medical officer. (c) **Copies of the test results shall be sent by the laboratory to the chief medical officer who made the decision under either Section 7511 or 7512 or who convened the panel under Section 7515 or 7516. The laboratory shall be responsible for protecting the confidentiality of these test results. Willful or negligent breach of this responsibility shall be grounds for a violation of the contract**. (d) The test results shall be sent by the chief medical officer to the designated recipients with the following disclaimer: "The tests were conducted in a medically approved manner but tests cannot determine exposure to or infection by AIDS or other communicable diseases with absolute accuracy. Persons receiving this test result should continue to monitor their own health and should consult a physician as appropriate." (e) **If the person subject to the test is a minor, copies of the test result shall also be sent to the minor's parents or guardian**. (f) **All persons, other than the test subject, who receive test results shall maintain the confidentiality of personal identifying data relating to the test results, except for disclosure which may be necessary to obtain medical or psychological care or advice, or to comply with this title.** (g) **The specimens and the results of the tests shall not be admissible evidence in any criminal or disciplinary proceeding.** (h) Any person performing testing, transmitting test results, or disclosing information in accordance with this title shall be immune from civil liability for any action undertaken in accordance with this title.		
H&S § 120820. Personal data; confidentiality	**HIV** **HIV data used in investigations, reports**	120820. (a) Personal data in any investigations, reports, and information relating thereto shall be kept confidential and be afforded protections provided by Section 100330, except as provided by Section 1603.1 or 1603.3. (b) **If patient-identifying information is subpoenaed from the department, the department shall seek and the court shall issue a protective order keeping this information confidential. The court order may require production, but limit the use and disclosure of, records, require production with names and identifying information deleted, provide sanctions for misuse of records or set forth other methods for assuring confidentiality**.		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
Health & Safety Code § 121010	**HIV blood test results** Disclosures of **HIV blood test results** to authorized persons	121010. Notwithstanding Section 120975 or 120980, **the results of a blood test to detect antibodies to the probable causative agent of AIDS may be disclosed to any of the following persons without written authorization of the subject of the test:** **(a) To the subject of the test or the subject's legal representative, conservator, or to any person authorized to consent to the test pursuant to subdivision (b) of Section 120990.** **(b) To a test subject's provider of health care, as defined in subdivision (d) of Section 56.05 of the Civil Code, except that for purposes of this section, "provider of health care" does not include a health care service plan regulated pursuant to Chapter 2.2 (commencing with Section 1340) of Division 2.** **(c) To an agent or employee of the test subject's provider of health care who provides direct patient care and treatment.** **(d) To a provider of health care who procures, processes, distributes, or uses a human body part donated pursuant to the Uniform Anatomical Gift Act (Chapter 3.5 (commencing with Section 7150) of Part 1 of Division 7).** **(e) (1) To the designated officer of an emergency response employee, and from that designated officer to an emergency response employee regarding possible exposure to HIV or AIDS, but only to the extent necessary to comply with provisions of the Ryan White Comprehensive AIDS Resources Emergency Act of 1990 (P.L. 101-381; 42 U.S.C. Sec. 201).** (2) For purposes of this subdivision, "designated officer" and "emergency response employee" have the same meaning as these terms are used in the Ryan White Comprehensive AIDS Resources Emergency Act of 1990 (P.L. 101-381; 42 U.S.C. Sec. 201). (3) The designated officer shall be subject to the confidentiality requirements specified in Section 120980, and may be personally liable for unauthorized release of any identifying information about the HIV results. Further, the designated officer shall inform the exposed emergency response employee that the employee is also subject to	121022. (a) To ensure knowledge of current trends in the HIV epidemic and to assure that California remains competitive for federal HIV and AIDS funding, health care providers and laboratories shall report cases of HIV infection to the local health officer using patient names. Local health officers shall report unduplicated HIV cases by name to the department. (b) The department and local health officers shall ensure continued reasonable access to anonymous HIV testing through alternative testing sites, as established by Section 120890, and in consultation with HIV planning groups and affected stakeholders, including representatives of persons living with HIV and health officers. (c) The department shall promulgate emergency regulations to conform the relevant provisions of Article 3.5 (commencing with Section 2641.5) of Chapter 4 of Title 17 of the California Code of Regulations, consistent with this chapter, within one year of the effective date of this section. (d) Pursuant to Section 121025, reported cases of HIV infection shall not be disclosed, discoverable, or compelled to be produced in any civil, criminal, administrative, or other proceeding. (e) State and local health department employees and contractors shall be required to sign confidentiality agreements developed by the department that include information related to the penalties for a breach of confidentiality, and the procedures for reporting a breach of confidentiality, prior to accessing confidential HIV-related public health records. Those agreements shall be reviewed annually by either the department or the appropriate local health department. (f) No person shall disclose identifying	• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		the confidentiality requirements specified in Section 120980, and may be personally liable for unauthorized release of any identifying information about the HIV test results.	information reported pursuant to subdivision (a) to the federal government, including, but not limited to, any agency, employee, agent, contractor, or anyone else acting on behalf of the federal government, except as permitted under subdivision (b) of Section 121025. (g) (1) Any potential or actual breach of confidentiality of HIV-related public health records shall be investigated by the local health officer, in coordination with the department, when appropriate. The local health officer shall immediately report any evidence of an actual breach of confidentiality of HIV-related public health records at a city or county level to the department and the appropriate law enforcement agency. (2) The department shall investigate any potential or actual breach of confidentiality of HIV-related public health records at the state level, and shall report any evidence of such a breach of confidentiality to an appropriate law enforcement agency. (h) Any willful, negligent, or malicious disclosure of cases of HIV infection reported pursuant to subdivision (a) shall be subject to the penalties prescribed in Section 121025. (i) Nothing in this section shall be construed to limit other remedies and protections available under state or federal law.	
Health & Safety Code § 121015- Disclosure to patient's spouse, sexual partner, needle sharer, or local health officer; physician liability; prohibition against compelled disclosure-	**HIV test results** Permitted HIV Positive test results disclosures to spouse, sexual partner, shared use of hypodermic needles, or to public health officer	121015. (a) Notwithstanding Section 120980 or any other provision of law, no physician and surgeon who has the results of a confirmed positive test to detect HIV infection of a patient under his or her care shall be held criminally or civilly liable for disclosing to a person reasonably believed to be the spouse, or to a person reasonably believed to be a sexual partner or a person with whom the patient has shared the use of hypodermic needles, or to the local health officer, that the patient has tested positive on a test to detect HIV infection, except that no physician and surgeon shall disclose any identifying information about the individual believed to be infected, except as required in Section 121022. (b) No physician and surgeon shall disclose the information described in subdivision (a) unless he or she has first discussed the test results with the patient and has offered		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		the patient appropriate educational and psychological counseling, that shall include information on the risks of transmitting the human immunodeficiency virus to other people and methods of avoiding those risks, and has attempted to obtain the patient's voluntary consent for notification of his or her contacts. The physician and surgeon shall notify the patient of his or her intent to notify the patient's contacts prior to any notification. When the information is disclosed to a person reasonably believed to be a spouse, or to a person reasonably believed to be a sexual partner, or a person with whom the patient has shared the use of hypodermic needles, the physician and surgeon shall refer that person for appropriate care, counseling, and followup. This section shall not apply to disclosures made other than for the purpose of diagnosis, care, and treatment of persons notified pursuant to this section, or for the purpose of interrupting the chain of transmission. (c) This section is permissive on the part of the attending physician, and all requirements and other authorization for the disclosure of test results to detect HIV infection are limited to the provisions contained in this chapter, Chapter 10 (commencing with Section 121075) and Sections 1603.1 and 1603.3. No physician has a duty to notify any person of the fact that a patient is reasonably believed to be infected with HIV, except as required by Section 121022. (d) The local health officer may alert any persons reasonably believed to be a spouse, sexual partner, or partner of shared needles of an individual who has tested positive on an HIV test about their exposure, without disclosing any identifying information about the individual believed to be infected or the physician making the report, and shall refer any person to whom a disclosure is made pursuant to this subdivision for appropriate care and followup. Upon completion of the local health officer's efforts to contact any person pursuant to this subdivision, all records regarding that person maintained by the local health officer pursuant to this subdivision, including, but not limited to, any individual identifying information, shall be expunged by the local health officer. (e) The local health officer shall keep confidential the identity and the seropositivity status of the individual tested and the identities of the persons contacted, as long as records of contacts are maintained. (f) Except as provided in Section 1603.1, 1603.3, or 121022, no person shall be compelled in any state, county, city, or local civil, criminal, administrative, legislative, or other proceedings to identify or provide identifying characteristics that would identify any individual reported or person contacted pursuant to this section.		
Health & Safety Code § 121025 - Personally identifying information confidentiality; disclosure; discovery; compelled production; penalties;	**HIV or AIDS Records** Disclosures by State or Local Public Health agencies of records relating to HIV or AIDS	121025. (a) **Public health records relating to human immunodeficiency virus (HIV) or acquired immunodeficiency syndrome (AIDS), containing personally identifying information, that were developed or acquired by state or local public health agencies, or an agent of such an agency, shall be confidential and shall not be disclosed, except as otherwise provided by law for public health purposes**		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
employment or insurance use		**or pursuant to a written authorization** by the person who is the subject of the record or by his or her guardian or conservator. (b) In accordance with subdivision (f) of **Section 121022, state or local public health agencies, or an agent of such an agency, may disclose personally identifying information in public health records, as described in subdivision (a), to other local, state, or federal public health agencies or to corroborating medical researchers, when the confidential information is necessary to carry out the duties of the agency or researcher in the investigation, control, or surveillance of disease, as determined by the state or local public health agency.** **(c) Any disclosure authorized by subdivision (a) or (b) shall include only the information necessary for the purpose of that disclosure and shall be made only upon agreement that the information will be kept confidential and will not be further disclosed without written authorization, as described in subdivision (a).** (d) No confidential public health record, as defined in subdivision (c) of Section 121035, shall be disclosed, discoverable, or compelled to be produced in any civil, criminal, administrative, or other proceeding. (e) (1) Any person who negligently discloses the content of any confidential public health record, as defined in subdivision (c) of Section 121035, to any third party, except pursuant to a written authorization, as described in subdivision (a), or as otherwise authorized by law, shall be subject to a civil penalty in an amount not to exceed two thousand five hundred dollars ($2,500), plus court costs, as determined by the court, which penalty and costs shall be paid to the person whose record was disclosed. (2) Any person who willfully or maliciously discloses the content of any confidential public health record, as defined in subdivision (c) of Section 121035, to any third party, except pursuant to a written authorization, or as otherwise authorized by law, shall be subject to a civil penalty in an amount not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), plus court costs, as determined by the court, which penalty and costs shall be paid to the person whose confidential public health record was disclosed. (3) Any person who willfully, maliciously, or negligently discloses the content of any confidential public health record, as defined in subdivision (c) of Section 121035, to any third party, except pursuant to a written authorization, or as otherwise authorized by		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		law, that results in economic, bodily, or psychological harm to the person whose confidential public health record was disclosed, is guilty of a misdemeanor, punishable by imprisonment in the county jail for a period not to exceed one year, or a fine of not to exceed twenty-five thousand dollars ($25,000), or both, plus court costs, as determined by the court, which penalty and costs shall be paid to the person whose confidential public health record was disclosed. (4) Any person who commits any act described in paragraph (1), (2), or (3), shall be liable to the person whose confidential public health record was disclosed for all actual damages for economic, bodily, or psychological harm that is a proximate result of the act. (5) Each violation of this section is a separate and actionable offense. (6) Nothing in this section limits or expands the right of an injured person whose confidential public health record was disclosed to recover damages under any other applicable law. (f) In the event that a confidential public health record, as defined in subdivision (c) of Section 121035, is disclosed, the information shall not be used to determine employability, or insurability of any person.		
Health & Safety Code § 121065-Testing	**HIV, hepatitis B, or hepatitis C status** Disclosures of medical information regarding the HIV, hepatitis B, or hepatitis C status of the source patient.	121065. (a) The withdrawal of blood shall be performed in a medically approved manner. Only a physician, registered nurse, licensed vocational nurse, licensed medical technician, or licensed phlebotomist may withdraw blood specimens for the purposes of this chapter. (b) The court shall order that the blood specimens be transmitted to a licensed medical laboratory and that tests be conducted thereon for medically accepted indications of exposure to or infection by HIV, hepatitis B, and hepatitis C. (c) (1) The test results shall be sent to the designated recipients with the following disclaimer: "The tests were conducted in a medically approved manner. Persons receiving this test result should continue to monitor their own health and should consult a physician as appropriate. Recipients of these test results are subject to existing confidentiality protections for any identifying information about HIV, hepatitis B, or hepatitis C test results. **Medical information regarding the HIV, hepatitis B, or hepatitis C status of the source patient shall be kept confidential and may not be further disclosed, except as otherwise authorized by law."** (2) The exposed individual shall also be informed of the penalties for disclosure for which he or she would be personally liable pursuant to Section 120980. If the person subject to the test is a minor, copies of the test result shall also be sent to the minor's parents or guardian. (d) The court shall order all persons, other than the test subject, who receive test results pursuant to Sections 121055, 121056, or 121060, to maintain the confidentiality of personal identifying data relating to the test results except for disclosure that may be		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		necessary to obtain medical or psychological care or advice. (e) The specimens and the results of tests ordered pursuant to Sections 121055, 121056, and 121060 shall not be admissible evidence in any criminal or juvenile proceeding. (f) Any person performing testing, transmitting test results, or disclosing information pursuant to the provisions of this chapter shall be immune from civil liability for any action undertaken in accordance with the provisions of this chapter.		
Insurance Code § 799.03. Testing for HIV or antibodies to HIV; informed consent; counseling; privacy protection; notification of positive test results	**HIV testing** An insurer that requests an applicant to take an HIV-related test shall obtain the applicant's written informed consent for the test and shall describe test, purpose, potential uses and limitations.	799.03. No insurer shall test for HIV or for the presence of antibodies to HIV for the purpose of determining insurability other than in accordance with the informed consent, counseling, and privacy protection provisions of this article and Article 6.6 (commencing with Section 791). Notwithstanding any other provision of law, this constitutes the exclusive requirements for counseling, informed consent, and privacy protection for that testing. (a) **An insurer that requests an applicant to take an HIV-related test shall obtain the applicant's written informed consent for the test. Written informed consent shall include a description of the test to be performed, including its purpose, potential uses, and limitations, the meaning of its results, procedures for notifying the applicant of the results, and the right to confidential treatment of the results. Prior to the applicant's execution of the consent, the insurer shall:** (1) Provide the applicant printed material describing HIV, its causes and symptoms, the manner in which it is spread, the test or tests used to detect HIV or the HIV antibody, and what a person can do whose test results are positive or negative. (2) Provide the applicant a list of counseling resources available, where the applicant can obtain assistance in understanding the meaning of the test and its results. The list may be provided from publicly available information. (b) The insurer shall notify an applicant of a positive test result by notifying the applicant's designated physician. If the applicant tested has not given written consent authorizing a physician to receive the test results, the applicant shall be urged, at the time the applicant is informed of the positive test results, o contact a private physician, the county department of health, the State Department of Health Services, local medical societies, or alternative test sites for appropriate counseling. (c) The commissioner shall develop and adopt standardized language for the informed consent disclosure form required by this section to be given to any applicant for life or disability income insurance who takes an HIV-related test.		• Consent • Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
Penal Code § 1202.6 - Prostitution; conviction; instruction in causes and consequences of AIDS; AIDS testing; report of test results; selection of program; testing procedure; confidentiality-	**AIDS testing** Confidentiality of AIDS testing for convicted persons.	1202.6. (a) Notwithstanding Sections 120975, 120980, and 120990 of the Health and Safety Code, upon the first conviction of any person for a violation of subdivision (b) of Section 647, the court shall, before sentencing or as a condition of probation, order the defendant to complete instruction in the causes and consequences of acquired immune deficiency syndrome (AIDS) pursuant to subdivision (d) and shall order the defendant to submit to testing for AIDS in accordance with subdivision (e). In addition, the court shall refer a defendant, where appropriate, to a program under Article 3.2 (commencing with Section 11320) of Chapter 2 of Part 3 of Division 9 of the Welfare and Institutions Code or to any drug diversion program, or both. (b) Upon a second or subsequent conviction of a violation of subdivision (b) of Section 647, the court shall, before sentencing, order the defendant to submit to testing for AIDS in accordance with subdivision (e). (c) At the sentencing hearing of a defendant ordered to submit to testing for AIDS pursuant to subdivision (a) or (b), the court shall furnish the defendant with a copy of the report submitted pursuant to subdivision (e) and shall direct the clerk to note the receipt of the report by the defendant in the records of the case. If the results of the test described in the report are positive, the court shall make certain that the defendant understands the nature and meaning of the contents of the report and shall further advise the defendant of the penalty established in Section 647f for a subsequent violation of subdivision (b) of Section 647. (d) The county health officer in each county shall select an agency, or agencies, in the county that shall provide AIDS prevention education. The county health officer shall endeavor to select an agency, or agencies, that currently provide AIDS prevention education programs to substance abusers or prostitutes. If no agency is currently providing this education, the county agency responsible for substance abuse shall develop an AIDS prevention education program either within the agency or under contract with a community-based, nonprofit organization in the county. The county health officer shall forward to the courts a list of agencies selected for purposes of referral. An AIDS prevention education program providing services, at a minimum, shall include details about the transmission of human immunodeficiency virus (HIV), the etiologic agent for AIDS, symptoms of AIDS or AIDS-related conditions, prevention through avoidance or cleaning of needles, sexual practices that constitute high risk, low risk, and no risk (including abstinence), and resources for assistance if the person decides to take a test for the etiologic agent for AIDS and receives a positive test result. The program also shall include other relevant medical and prevention information as it becomes available. (e) The court shall order testing of every defendant as ordered pursuant to subdivision (a) or (b) for evidence of antibodies to the probable causative agent of acquired immune deficiency syndrome. Notwithstanding Section 120980 of the Health and Safety Code, written copies of the report on the test shall be furnished to both of	The State Department of Health Services shall maintain the confidentiality of the reports received pursuant to subdivision (e), except that the department shall furnish copies of any report to a district attorney upon request.	• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		the following: (1) The court in which the defendant is to be sentenced. (2) The State Department of Health Services. (f) Except as provided in subdivisions (c) and (g), the reports required by subdivision (e) shall be confidential. (g) **The State Department of Health Services shall maintain the confidentiality of the reports received pursuant to subdivision (e), except that the department shall furnish copies of any report to a district attorney upon request.**		
WIC § 4135. Mentally abnormal sex offender; commitment; discharge; records; inspection	**Mental Health** Confidentiality of State Department of Mental Health committed mentally abnormal sex offenders.	Any person committed to the State Department of Mental Health as a mentally abnormal sex offender shall remain a patient committed to the department for the period specified in the court order of commitment or until discharged by the medical director of the state hospital in which the person is a patient, whichever occurs first. The medical director may grant such patient a leave of absence upon such terms and conditions as the medical director deems proper. **The petition for commitment of a person as a mentally abnormal sex offender, the reports, the court orders and other court documents filed in the court in connection therewith shall not be open to inspection by any other than the parties to the proceeding, the attorneys for the party or parties, and the State Department of Mental Health, except upon the written authority of a judge of the superior court of the county in which the proceedings were had. Records of the supervision, care and treatment given to each person committed to the State Department of Mental Health as a mentally abnormal sex offender shall not be open to the inspection of any person not in the employ of the department or of the state hospital, except that a judge of the superior court may by order permit examination of such records.** The charges for the care and treatment rendered to persons committed as mentally abnormal sex offenders shall be in accordance with the provisions of Article 4 (commencing with Section 7275) of Chapter 3 of Division 7.		• Collection, Request, Use, & Disclosure
WIC LPS § 5202. Pre-petition screening; report of findings	**Mental health** County/state mental health prepetition screening information	The person or agency designated by the county shall prepare the petition and all other forms required in the proceeding, and shall be responsible for filing the petition. Before filing the petition, the person or agency designated by the county shall request the person or agency designated by the county and approved by the State Department of Mental Health to provide prepetition screening to determine whether there is probable cause to believe the allegations. The person or agency providing prepetition screening shall conduct a reasonable investigation of the allegations and make a reasonable effort to personally interview the subject of the petition. The screening shall also determine whether the person will agree voluntarily to receive crisis intervention services or an evaluation in his own home or in a facility designated by the county and		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		approved by the State Department of Mental Health. Following prepetition screening, the person or agency designated by the county shall file the petition if satisfied that there is probable cause to believe that the person is, as a result of mental disorder, a danger to others, or to himself or herself, or gravely disabled, and that the person will not voluntarily receive evaluation or crisis intervention. If the petition is filed, it shall be accompanied by a report containing the findings of the person or agency designated by the county to provide prepetition screening. **The prepetition screening report submitted to the superior court shall be confidential and shall be subject to the provisions of Section 5328.**		
WIC LPS § 5328. Confidential information and records; disclosure; consent	**Mental health** All information and records for services rendered by State hospitals/community mental health clinics	All information and records obtained in the course of providing services under Division 4 (commencing with Section 4000), Division 4.1 (commencing with Section 4400), Division 4.5 (commencing with Section 4500), Division 5 (commencing with Section 5000), Division 6 (commencing with Section 6000), or Division 7 (commencing with Section 7100), to either voluntary or involuntary recipients of services shall be confidential. Information and records obtained in the course of providing similar services to either voluntary or involuntary recipients prior to 1969 shall also be confidential. **Information and records shall be disclosed only in any of the following cases**:…) http://law.onecle.com/california/welfare/5328.html		• Collection, Request, Use, & Disclosure
WIC LPS § 5328.01. Confidential information and records; disclosure to law enforcement agencies; consent; court orders	**Mental health** Disclosures to governmental law enforcement agencies investigating evidence of a crime where the records relate to a patient who is confined or has been confined as a mentally disordered sex offender.	Notwithstanding Section 5328**, all information and records made confidential under the first paragraph of Section 5328 shall also be disclosed to governmental law enforcement agencies investigating evidence of a crime where the records relate to a patient who is confined or has been confined as a mentally disordered sex offender** or pursuant to Section 1026 or 1368 of the Penal Code and the records are in the possession or under the control of any state hospital serving the mentally disabled, as follows: (a) In accordance with the written consent of the patient; or (b) If authorized by an appropriate order of a court of competent jurisdiction in the county where the records are located compelling a party to produce in court specified records and specifically describing the records being sought, when the order is granted after an application showing probable cause therefore. In assessing probable cause, the court shall do all of the following: (1) Weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services. (2) Determine that there is a reasonable likelihood that the records in question will disclose material information or evidence of substantial value in connection with the investigation or prosecution.		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		(3) Determine that the crime involves the causing of, or direct threatening of, the loss of life or serious bodily injury. (4) In granting or denying a subpoena, the court shall state on the record the reasons for its decision and the facts which the court considered in making such a ruling. (5) If a court grants an order permitting disclosure of such records, the court shall issue all orders necessary to protect, to the maximum extent possible, the patient's privacy and the privacy and confidentiality of the physician-patient relationship. (6) Any records disclosed pursuant to the provisions of this subdivision and any copies thereof shall be returned to the facility at the completion of the investigation or prosecution unless they have been made a part of the court record. (c) A governmental law enforcement agency applying for disclosure of patient records under this subdivision may petition the court for an order, upon a showing of probable cause to believe that delay would seriously impede the investigation, which requires the ordered party to produce the records forthwith. (d) Records obtained by a governmental law enforcement agency pursuant to this section shall not be disseminated to any other agency or person unless such dissemination relates to the criminal investigation for which the records were obtained by the governmental law enforcement agency. The willful dissemination of any record in violation of this paragraph shall constitute a misdemeanor. (e) If any records obtained pursuant to this section are of a patient presently receiving treatment at the state hospital serving the mentally disabled, the law enforcement agency shall only receive copies of the original records.		
WIC LPS § 5328.02. Confidential information and records; disclosure to youth authority and adult correctional agency	**Mental health** Disclosures of mental health information to the Youth Authority and Adult Correctional Agency	Notwithstanding Section 5328, all information and records made confidential under the first paragraph of Section 5328 shall also be disclosed to the Youth Authority and Adult Correctional Agency or any component thereof, as necessary to the administration of justice.		• Collection, Request, Use, & Disclosure
WIC LPS § 5328.1. Information to patient's family; patient authorization; liability for damages	**Mental health** Disclosures to members of the family of mental health patient	(a) **Upon request of a member of the family of a patient, or other person designated by the patient, a public or private treatment facility shall give the family member or the designee notification of the patient's diagnosis, the prognosis, the medications prescribed, the side effects of medications prescribed, if any, and the progress of the patient, if, after notification of the patient that this information is requested, the patient authorizes its disclosure**. If, when initially informed of the request for notification, the patient is unable to authorize the release of such information, notation of the attempt shall be made into the patient's treatment record, and daily efforts shall be made to secure the patient's consent or refusal of authorization. However, if a request for information is made by the spouse, parent, child, or sibling of the patient and the patient is unable to authorize the release of such information, the requester shall be given notification of the patient's presence in		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		the facility, except to the extent prohibited by federal law. (b) Upon the admission of any mental health patient to a 24-hour public or private health facility licensed pursuant to Section 1250 of the Health and Safety Code, the facility shall make reasonable attempts to notify the patient's next of kin or any other person designated by the patient, of the patient's admission, unless the patient requests that this information not be provided. The facility shall make reasonable attempts to notify the patient's next of kin or any other person designated by the patient, of the patient's release, transfer, serious illness, injury, or death only upon request of the family member, unless the patient requests that this information not be provided. The patient shall be advised by the facility that he or she has the right to request that this information not be provided. (c) No public or private entity or public or private employee shall be liable for damages caused or alleged to be caused by the release of information or the omission to release information pursuant to this section. Nothing in this section shall be construed to require photocopying of a patient's medical records in order to satisfy its provisions.		
WIC LPS § 5328.15. Authorized disclosure of confidential information and records	**Mental health** Disclosures of mental health information for licensing purposes	All information and records obtained in the course of providing services under Division 5 (commencing with Section 5000), Division 6 (commencing with Section 6000), or Division 7 (commencing with Section 7000), to either voluntary or involuntary recipients of services shall be confidential**. Information and records may be disclosed, however, notwithstanding any other provision of law, as follows:** **(a) To authorized licensing personnel who are employed by, or who are authorized representatives of, the State Department of Health Services, and who are licensed or registered health professionals, and to authorized legal staff or special investigators who are peace officers who are employed by, or who are authorized representatives of the State Department of Social Services, as necessary to the performance of their duties to inspect, license, and investigate health facilities and community care facilities and to ensure that the standards of care and services provided in such facilities are adequate and appropriate and to ascertain compliance with the rules and regulations to which the facility is subject.** The confidential information shall remain confidential except for purposes of inspection, licensing, or investigation pursuant to Chapter 2 (commencing with Section 1250) of, and Chapter 3 (commencing with Section 1500) of, Division 2 of the Health and Safety Code, or a criminal, civil, or administrative proceeding in relation thereto. The confidential information may be used by the State Department of Health Services or the State Department of Social Services in a criminal, civil, or administrative proceeding. The confidential information shall be available only to the judge or hearing officer and to the parties to the case. Names which are confidential shall be listed in attachments separate to the general pleadings. The confidential information shall be sealed after the conclusion of the criminal, civil, or administrative hearings, and shall		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		not subsequently be released except in accordance with this subdivision. If the confidential information does not result in a criminal, civil, or administrative proceeding, it shall be sealed after the State Department of Health Services or the State Department of Social Services decides that no further action will be taken in the matter of suspected licensing violations. Except as otherwise provided in this subdivision, confidential information in the possession of the State Department of Health Services or the State Department of Social Services shall not contain the name of the patient. (b) To any board which licenses and certifies professionals in the fields of mental health pursuant to state law, when the Director of Mental Health has reasonable cause to believe that there has occurred a violation of any provision of law subject to the jurisdiction of that board and the records are relevant to the violation. This information shall be sealed after a decision is reached in the matter of the suspected violation, and shall not subsequently be released except in accordance with this subdivision. Confidential information in the possession of the board shall not contain the name of the patient.		
WIC LPS 5328.4. Crimes against person by or upon patient; release of information	**Mental health** Disclosures of mental health information to governmental law enforcement agencies	**The physician in charge of the patient, or the professional person in charge of the facility or his or her designee, when he or she has probable cause to believe that a patient while hospitalized has committed, or has been the victim of, murder, manslaughter, mayhem, aggravated mayhem, kidnapping, carjacking, robbery, assault with intent to commit a felony, arson, extortion, rape, forcible sodomy, forcible oral copulation, unlawful possession of a weapon as provided in Section 12020 of the Penal Code, or escape from a hospital by a mentally disordered sex offender as provided in Section 6330 of the Welfare and Institutions Code, shall release information about the patient to governmental law enforcement agencies**. The physician in charge of the patient, or the professional person in charge of the facility or his or her designee, when he or she has probable cause to believe that a patient, while hospitalized has committed, or has been the victim of assault or battery may release information about the patient to governmental law enforcement agencies. This section shall be limited solely to information directly relating to the factual circumstances of the commission of the enumerated offenses and shall not include any information relating to the mental state of the patient or the circumstances of his or her voluntary or involuntary admission, commitment, or treatment. This section shall not be construed as an exception to or in any other way affecting the provisions of Article 7 (commencing with Section 1010) of Chapter 4 of Division 8 of the Evidence Code.		• Collection, Request, Use, & Disclosure
WIC LPS 5328.5. Confidential information and records; disclosure; elder abuse or dependent adult abuse	**Mental health** Disclosure of mental health information for prevention, investigation, treatment of elder abuse.	**Information and records described in Section 5328 may be disclosed in communications relating to the prevention, investigation, or treatment of elder abuse or dependent adult abuse** pursuant to Chapter 11 (commencing with Section 15600) and Chapter 13 (commencing with Section 15750), of Part 3 of Division 9.		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
WIC LPS 5328.7. Consent forms; record of forms used; copy for patient	**Mental health** State Department of Mental Health consent, use, and disclosure	**Signed consent forms by a patient for release of any information to which such patient is required to consent under the provisions of Sections 11878 or 11879 of the Health and Safety Code or subdivision (a) or (d) of Section 5328 shall be obtained for each separate use with the use specified, the information to be released, the name of the agency or individual to whom information will be released indicated on the form and the name of the responsible individual who has authorization to release information specified. Any use of this form shall be noted in the patient file. Patients who sign consent forms shall be given a copy of the consent form signed**.		• Collection, Request, Use, & Disclosure • Consent
WIC LPS § 5328.8. Death of patient in state mental hospital; release of information to coroner	**Mental health** Disclosures of mental health information by State Department of Mental Health to the coroner	The State Department of Mental Health, the physician in charge of the patient, or the professional person in charge of the facility or his or her designee, shall, except as otherwise provided in this section, release information obtained in the course of providing services under Division 5 (commencing with Section 5000), Division 6 (commencing with Section 6000), or Division 7 (commencing with Section 7100), to the coroner when a patient dies from any cause, natural or otherwise, while hospitalized in a state mental hospital. The State Department of Mental Health, the physician in charge of the patient, or the professional person in charge of the facility or his or her designee, shall not release any notes, summaries, transcripts, tapes, or records of conversations between the patient and health professional personnel of the hospital relating to the personal life of the patient which is not related to the diagnosis and treatment of the patient's physical condition. Any information released to the coroner pursuant to this section shall remain confidential and shall be sealed and shall not be made part of the public record.		• Collection, Request, Use, & Disclosure
WIC LPS 5328.9. Disclosure to employer; conditions; disclosure to patient; notice of nondisclosure to superior court	**Mental health** Disclosure of mental health information to qualified physician/psychiatrist representing employer.	**If at such time as a patient's hospital records are required by an employer to whom the patient has applied for employment, such records shall be forwarded to a qualified physician or psychiatrist representing the employer upon the request of the patient unless the physician or administrative officer responsible for the patient deems the release of such records contrary to the best interest of the patient.** If the physician or administrative officer responsible for a patient deems the release of such records contrary to the best interest of the patient, he shall notify the patient within five days. In the event that the disclosure of the patient's records to the patient himself would not serve his best interests, the physician or administrative officer in question shall render formal notice of his decision to the superior court of the county in which the patient resides.		• Collection, Request, Use, & Disclosure
WIC LPS § 5541. Authorization; revocation; inspection and copying of information and records	**Mental health** Access to mental health information by patients' rights advocate.	a) **A specific authorization by the client or by the guardian ad litem is necessary for a county patients' rights advocate to have access to, copy or otherwise use confidential records or information pertaining to the client.** Such an authorization shall be given knowingly and voluntarily by a client or guardian ad litem and shall be in		• Collection, Request, Use, & Disclosure • Access to Information

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		writing or be reduced to writing. The client or the guardian ad litem, whoever has entered into the agreement, may revoke such authorization at any time, either in writing or by oral declaration to the advocate. (b) When specifically authorized by the client or the guardian ad litem, the county patients' rights advocate may inspect and copy confidential client information and records.		
Health & Safety 123115. Representative of minor; mental health records	**Mental Health & Minors** Access to information related to mental health of minors	123115. (a) The **representative of a minor shall not be entitled to inspect or obtain copies of the minor's patient records in either of the following circumstances: (1) With respect to which the minor has a right of inspection under Section 123110.** **(2) Where the health care provider determines that access to the patient records requested by the representative would have a detrimental effect on the provider's professional relationship with the minor patient or the minor's physical safety or psychological well-being**. The decision of the health care provider as to whether or not a minor's records are available for inspection or copying under this section shall not attach any liability to the provider, unless the decision is found to be in bad faith. (b) **When a health care provider determines there is a substantial risk of significant adverse or detrimental consequences to a patient in seeing or receiving a copy of mental health records requested by the patient**, the provider may decline to permit inspection or provide copies of the records to the patient, subject to the following conditions: (1) The health care provider shall make a written record, to be included with the mental health records requested, noting the date of the request and explaining the health care provider's reason for refusing to permit inspection or provide copies of the records, including a description of the specific adverse or detrimental consequences to the patient that the provider anticipates would occur if inspection or copying were permitted. (2) The health care provider shall permit inspection by, or provide copies of the mental health records to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, or licensed clinical social worker, designated by request of the patient. Any marriage and family therapist registered intern, as defined in Chapter 13 (commencing with Section 4980) of Division 2 of the Business and Professions Code, may not inspect the patient's mental health records or obtain copies thereof, except pursuant to the direction or supervision of a licensed professional specified in subdivision (f) of Section 4980.40 of the Business and Professions Code. Prior to providing copies of mental health records to a marriage and family therapist registered intern, a receipt for those records shall be signed by the supervising licensed professional. The licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, licensed clinical social worker, or marriage and family		Access

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		therapist registered intern to whom the records are provided for inspection or copying shall not permit inspection or copying by the patient. (3) The health care provider shall inform the patient of the provider's refusal to permit him or her to inspect or obtain copies of the requested records, and inform the patient of the right to require the provider to permit inspection by, or provide copies to, a licensed physician and surgeon, licensed psychologist, licensed marriage and family therapist, or licensed clinical social worker, designated by written authorization of the patient. (4) The health care provider shall indicate in the mental health records of the patient whether the request was made under paragraph (2).		
"A minor may consent to medical care related to the prevention or treatment of pregnancy," except sterilization. Cal. Family Code § 6925	**Minors** Minor consent for care to prevent or treat pregnancy, except sterilization	6925. (a) A minor may consent to medical care related to the prevention or treatment of pregnancy. (b) This section does not authorize a minor: (1) To be sterilized without the consent of the minor's parent or guardian. (2) To receive an abortion without the consent of a parent or guardian other than as provided in Section 123450 of the Health and Safety Code.		• Consent
A minor may consent to an abortion without parental consent and without court permission. (American Academy of Pediatrics v. Lungren 16 Cal.4th 307 (1997)).	**Minors** Minor consent to an abortion	The **health care provider is not permitted to inform a parent or legal guardian without minor's consent. The provider can only share the minor's medical records with the signed consent of the minor**. (Cal. Health & Safety Code §§ 123110(a), 123115(a); Cal. Civ. 56.10, 56.11).		• Consent
A minor who has a condition or injury which is considered an emergency but whose parent or guardian is unavailable to give consent is permitted to give consent for medical services. (Cal. Business and Professions Code § 2397).	**Minors** Emergency consent for minor	(a) A licensee shall not be liable for civil damages for injury or death caused in an emergency situation occurring in the licensee's office or in a hospital on account of a failure to inform a patient of the possible consequences of a medical procedure where the failure to inform is caused by any of the following: (1) The patient was unconscious. (2) **The medical procedure was undertaken without the consent of the patient because the licensee reasonably believed that a medical procedure should be undertaken immediately and that there was insufficient time to fully inform the patient**. (3) A medical procedure was performed on a person legally incapable of giving consent, and the licensee reasonably believed that a medical procedure should be undertaken immediately and that there was insufficient time to obtain the informed consent of a person authorized to give such consent for the patient. (b) This section is applicable only to actions for damages for injuries or death arising because of a licensee's failure to inform, and not to actions for damages arising	The health care provider shall inform the minor's parent or guardian.	• Consent

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		because of a licensee's negligence in rendering or failing to render treatment. (c) As used in this section: (1) "Hospital" means a licensed general acute care hospital as defined in subdivision (a) of Section 1250 of the Health and Safety Code. (2) "Emergency situation occurring in the licensee's office" means a situation occurring in an office, other than a hospital, used by a licensee for the examination or treatment of patients, requiring immediate services for alleviation of severe pain, or immediate diagnosis and treatment of unforeseeable medical conditions, which, if not immediately diagnosed and treated, would lead to serious disability or death. (3) "Emergency situation occurring in a hospital" means a situation occurring in a hospital, whether or not it occurs in an emergency room, requiring immediate services for alleviation of severe pain, or immediate diagnosis and treatment of unforeseeable medical conditions, which, if not immediately diagnosed and treated, would lead to serious disability or death. (d) Nothing in this article shall be construed to authorize practice by a podiatrist beyond that set forth in Section 2473.		
"A minor may consent to the minor's medical care or dental care (Cal. Fam. Code § 6922(a)).	**Minors** Minor's consent for medical or dental care	6922. (a) **A minor may consent to the minor's medical care or dental care** if all of the following conditions are satisfied: (1) The minor is 15 years of age or older. (2) The minor is living separate and apart from the minor's parents or guardian, whether with or without the consent of a parent or guardian and regardless of the duration of the separate residence. (3) The minor is managing the minor's own financial affairs, regardless of the source of the minor's income.	"A physician and surgeon or dentist MAY, with or without the consent of the minor patient, advise the minor's parent or guardian of the treatment given or needed if the physician and surgeon or dentist has reason to know, on the basis of the information given by the minor, the whereabouts of the parent or guardian." (Cal. Fam. Code § 6922(c)).	• Consent
"A minor who is 12 years of age or older may consent to mental health treatment or counseling on an outpatient basis, or to residential shelter services, if both of the following requirements are satisfied: (1) The minor, in the opinion of the attending professional person, is mature enough to participate intelligently in the outpatient services or residential shelter services. (2) The minor (A) would present a danger of	**Minors** A minor who is 12 years of age or older may consent to mental health treatment or counseling on an outpatient basis, or to residential shelter services	(a) As used in this section: (1) "Mental health treatment or counseling services" means the provision of mental health treatment or counseling on an outpatient basis by any of the following: (A) A governmental agency. (B) A person or agency having a contract with a governmental agency to provide the services. (C) An agency that receives funding from community united funds. (D) A runaway house or crisis resolution center. (E) A professional person, as defined in paragraph (2). (2) "Professional person" means any of the following: (A) A person designated as a mental health professional in Sections 622 to 626,	MENTAL HEALTH TREATMENT: The health care provider is required to involve a parent or guardian unless the health care provider decides that involvement is inappropriate. This decision must be documented in the minor's record.	• Consent

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
serious physical or mental harm to self or to others without the mental health treatment or counseling or residential shelter services, or (B) is the alleged victim of incest or child abuse." (Cal. Family Code § 6924).		inclusive, of Article 8 of Subchapter 3 of Chapter 1 of Title 9 of the California Code of Regulations. (B) A marriage and family therapist as defined in Chapter 13 (commencing with Section 4980) of Division 2 of the Business and Professions Code. (C) A licensed educational psychologist as defined in Article 5 (commencing with Section 4986) of Chapter 13 of Division 2 of the Business and Professions Code. (D) A credentialed school psychologist as described in Section 49424 of the Education Code. (E) A clinical psychologist as defined in Section 1316.5 of the Health and Safety Code. (F) The chief administrator of an agency referred to in paragraph (1) or (3). (G) A marriage and family therapist registered intern, as defined in Chapter 13 (commencing with Section 4980) of Division 2 of the Business and Professions Code, while working under the supervision of a licensed professional specified in subdivision (f) of Section 4980.40 of the Business and Professions Code. (3) "Residential shelter services" means any of the following: (A) The provision of residential and other support services to minors on a temporary or emergency basis in a facility that services only minors by a governmental agency, a person or agency having a contract with a governmental agency to provide these services, an agency that receives funding from community funds, or a licensed community care facility or crisis resolution center. (B) The provision of other support services on a temporary or emergency basis by any professional person as defined in paragraph (2). (b) **A minor who is 12 years of age or older may consent to mental health treatment or counseling on an outpatient basis, or to residential shelter services**, if both of the following requirements are satisfied: (1) The minor, in the opinion of the attending professional person, is mature enough to participate intelligently in the outpatient services or residential shelter services. (2) The minor (A) would present a danger of serious physical or mental harm to self or to others without the mental health treatment or counseling or residential shelter services, or (B) is the alleged victim of incest or child abuse. (c) A professional person offering residential shelter services, whether as an individual or as a representative of an entity specified in paragraph (3) of subdivision (a), shall make his or her best efforts to notify the parent or guardian of the provision of services. (d) **The mental health treatment or counseling of a minor authorized by this section shall include involvement of the minor's parent or guardian unless, in the opinion of the professional person who is treating or counseling the minor, the**		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		involvement would be inappropriate. The professional person who is treating or counseling the minor shall state in the client record whether and when the person attempted to contact the minor's parent or guardian, and whether the attempt to contact was successful or unsuccessful, or the reason why, in the professional person's opinion, it would be inappropriate to contact the minor's parent or guardian. (e) The minor's parents or guardian are not liable for payment for mental health treatment or counseling services provided pursuant to this section unless the parent or guardian participates in the mental health treatment or counseling, and then only for services rendered with the participation of the parent or guardian. The minor's parents or guardian are not liable for payment for any residential shelter services provided pursuant to this section unless the parent or guardian consented to the provision of those services. (f) This section does not authorize a minor to receive convulsive therapy or psychosurgery as defined in subdivisions (f) and (g) of Section 5325 of the Welfare and Institutions Code, or psychotropic drugs without the consent of the minor's parent or guardian.		
"A minor who is 12 years of age or older and who is alleged to have been raped may consent to medical care related to the diagnosis or treatment of the condition and the collection of medical evidence with regard to the alleged rape." (Cal. Family Code 6927).	**Minors** **Minor's consent for medical treatment related to rape**	6927**. A minor who is 12 years of age or older and who is alleged to have been raped may consent to medical care related to the diagnosis or treatment of the condition and** the collection of medical evidence with regard to the alleged rape.	The health care provider is not permitted to inform a parent or legal guardian without minor's consent. The provider can only share the minor's medical records with the signed consent of the minor. (Cal. Health & Safety Code §§ 123110(a), 123115(a); Cal. Civ. 56.10, 56.11).	• Consent
A minor who may have been sexually assaulted or raped may consent to medical care related to the diagnosis, treatment and the collection of medical evidence. (Cal. Family Code § 6928).	**Minors** Provision of consent to minor's medical care in relation to alleged sexual assault	6928. (a) "Sexually assaulted" as used in this section includes, but is not limited to, conduct coming within Section 261, 286, or 288a of the Penal Code. (b) **A minor who is alleged to have been sexually assaulted may consent to medical care related to the diagnosis and treatment of the condition, and the collection of medical evidence with regard to the alleged sexual assault**. (c) **The professional person providing medical treatment shall attempt to contact the minor's parent or guardian and shall note in the minor's treatment record the date and time the professional person attempted to contact the parent or guardian and whether the attempt was successful or unsuccessful.** This subdivision does not apply if the professional person reasonably believes that the minor's parent or guardian committed the sexual assault on the minor.	The health care provider must attempt to contact the minor's parent/guardian and must note the day and time of the attempted contact and whether it was successful. This provision does not apply if the treating professional reasonably believes that the parent/guardian committed the rape or assault.	• Consent
"A minor who is 12 years of age or older may consent to medical	**Minors**	(b) A minor who is 12 years of age or older may consent to medical care and counseling relating to the diagnosis and treatment of a drug- or alcohol-related	Federal law prohibits programs from disclosing information without a minor's	• Consent

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
care and counseling relating to the diagnosis and treatment of a drug or alcohol related problem."(Cal. Family Code §6929(b)).	Consent for diagnosis and treatment by minor's with drug or alcohol-related problems	problem.	written consent UNLESS: 1) the disclosure is limited to information that will reduce a threat of physical harm against an individual AND 2) the program director has determined that the minor is incapable of making a rational decision about such disclosure. (42 C.F.R. §2.14). For example, programs may not reveal urinalysis results or confirm program enrollment. (42 C.F.R. §2.11; US v Eide, 875 F.2d 1429, 1435 (9th Cir. 1989)). This law only applies to: 1) federally assisted programs dedicated to providing substance abuse services, or 2) staff members or units specifically dedicated to providing substance abuse services at federally assisted medical facilities (42 C.F.R. §2.11; See 42 C.F.R. §2.12 for more). Federally assisted programs are defined as programs authorized, certified, licensed or funded by the federal government. Examples include programs that are: receiving tax deductible donations; tax exempt; receiving any federal operating funds; or registered with Medicare. (42 C.F.R. §2.12). For programs that don't meet this criteria, state law applies. State law allows health care providers to determine whether involving a parent or guardian in the minor's treatment would be appropriate. This decision must be documented in the minor's record. (Cal. Family Code §6929(c)). A provider shall not be liable for any good faith decisions concerning access to a minor's records. (Cal. Health & Safety Code §123115(a)(2); See generally 42 U.S.C.	
A minor 12 and older is competent to give written consent for an HIV test. (Cal.	**Minors** **Minor's consent for HIV test**	(a) (1) When the subject of an HIV test is not competent to give consent for the test to be performed, written consent for the test may be obtained from the subject's parents, guardians, conservators, or other person lawfully authorized to make health care	The health care provider is not permitted to inform a parent or legal guardian without minor's consent. The provider can only share	• Consent

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
Health and Safety Code § 121020).		decisions for the subject. **For purposes of this paragraph, a minor shall be deemed not competent to give consent if he or she is under 12 years of age**. (2) Notwithstanding paragraph (1), when the subject of the test is a minor adjudged to be a dependent child of the court pursuant to Section 360 of the Welfare and Institutions Code, written consent for the test to be performed may be obtained from the court pursuant to its authority under Section 362 or 369 of the Welfare and Institutions Code. (b) Written consent shall only be obtained for the subject pursuant to subdivision (a) when necessary to render appropriate care or to practice preventative measures. (c) The person authorized to consent to the test pursuant to subdivision (a) shall be permitted to do any of the following: (1) Notwithstanding Sections 120975 and 120980, receive the results of the test on behalf of the subject without written authorization. (2) Disclose the test results on behalf of the subject in accordance with Sections 120975 and 120980. (3) Provide written authorization for the disclosure of the test results on behalf of the subject in accordance with Sections 120975 and 120980.	the minor's medical records with the signed consent of the minor. (Cal. Health & Safety Code §§ 123110(a), 123115(a); Cal. Civ. 56.10, 56.11). DIAGNOSIS AND/OR TREATMENT FOR INFECTIOUS, CONTAGIOUS COMMUNICABLE DISEASE, AND SEXUALLY TRANSMITTED DISEASES Adolescent Provider Toolkit A-1 © Adolescent Health Working Group, 2003	
"A physician and surgeon or dentist or their agents . . . may take skeletal X-rays of the child without the consent of the child's parent or guardian, but only for purposes of diagnosing the case as one of possible child abuse or neglect and determining the extent of." (Cal Penal Code § 11171).	**Child abuse** Victims of child physical abuse or neglect	a) (1) The Legislature hereby finds and declares that adequate protection of victims of child physical abuse or neglect has been hampered by the lack of consistent and comprehensive medical examinations. (2) Enhancing examination procedures, documentation, and evidence collection relating to child abuse or neglect will improve the investigation and prosecution of child abuse or neglect as well as other child protection efforts. (b) The agency or agencies designated by the Director of Finance pursuant to Section 13820 shall, in cooperation with the State Department of Social Services, the Department of Justice, the California Association of Crime Lab Directors, the California District Attorneys Association, the California State Sheriffs Association, the California Peace Officers Association, the California Medical Association, the California Police Chiefs' Association, child advocates, the California Medical Training Center, child protective services, and other appropriate experts, establish medical forensic forms, instructions, and examination protocols for victims of child physical abuse or neglect using as a model the form and guidelines developed pursuant to Section 13823.5. (c) The forms shall include, but not be limited to, a place for notation concerning each of the following: (1) Any notification of injuries or any report of suspected child physical abuse or neglect to law enforcement authorities or children's protective services, in accordance with existing reporting procedures. (2) Addressing relevant consent issues, if indicated.	Neither the physician-patient privilege nor the psychotherapist-patient privilege applies to information reported pursuant to this law in any court proceeding.	

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		(3) The taking of a patient history of child physical abuse or neglect that includes other relevant medical history. (4) The performance of a physical examination for evidence of child physical abuse or neglect. (5) The collection or documentation of any physical evidence of child physical abuse or neglect, including any recommended photographic procedures. (6) The collection of other medical or forensic specimens, including drug ingestion or toxication, as indicated. (7) Procedures for the preservation and disposition of evidence. (8) Complete documentation of medical forensic exam findings with recommendations for diagnostic studies, including blood tests and X-rays. (9) An assessment as to whether there are findings that indicate physical abuse or neglect. (d) **The forms shall become part of the patient's medical record pursuant to guidelines established by the advisory committee of the agency or agencies designated by the Director of Finance pursuant to Section 13820 and subject to the confidentiality laws pertaining to the release of a medical forensic examination records**. (e) The forms shall be made accessible for use on the Internet.		
WIC 4903. Access to information and records; confidentiality of records of agency	**Persons with disabilities** Authorization of access to information regarding persons with disabilities to protection and advocacy agencies.	(1) Any person who is a client of the agency, or any person who has requested assistance from the agency, if that person or the agent designated by that person, or the legal guardian, conservator, or other legal representative of that person, has authorized the protection and advocacy agency to have access to the records and information. **If a person with a disability who is able to authorize the protection and advocacy agency to access his or her records expressly denies this access after being informed by the protection and advocacy agency of his or her right to authorize or deny access, the protection and advocacy agency may not have access to that person's records** (2) Any person, including any individual who cannot be located, to whom all of the following conditions apply: (A) The individual, due to his or her mental or physical condition, is unable to authorize the protection and advocacy agency to have access to his or her records. (B) The individual does not have a legal guardian, conservator, or other legal		• Collection, Request, Use, & Disclosure • Access to Information

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		representative, or the individual's representative is a public entity, including the state or one of its political subdivisions. (C) The protection and advocacy agency has received a complaint that the individual has been subject to abuse or neglect, or has determined that probable cause exists to believe that the individual as been subject to abuse or neglect. (3) Any person who is deceased, and for whom the protection and advocacy agency has received a complaint that the individual had been subjected to abuse or neglect, or for whom the agency has determined that probable cause exists to believe that the individual had been subjected to abuse or neglect. (4) Any person who has a legal guardian, conservator, or other legal representative with respect to whom a complaint has been received by the protection and advocacy agency, or with respect to whom the protection and advocacy agency has determined that probable cause exists to believe that the person has been subjected to abuse or neglect, whenever all of the following conditions exist: (A) The representative has been contacted by the protection and advocacy agency upon receipt of the representative's name and address. (B) The protection and advocacy agency has offered assistance to the representatives to resolve the situation. (C) The representative has failed or refused to act on behalf of the person. (b) Individual records that shall be available to the protection and advocacy agency under this section shall include, but not be limited to, all of the following information and records related to the investigation, whether written or in another medium, draft or final, including, but not limited to, handwritten notes, electronic files, photographs, videotapes, or audiotapes: (1) Information and records prepared or received in the course of providing intake, assessment, evaluation, education, training, or other supportive services, including, but not limited to, medical records, financial records, monitoring reports, or other reports, prepared or received by a member of the staff of a facility, program, or service that is providing care, treatment, or services. (2) Reports prepared by an agency charged with investigating reports of incidents of abuse, neglect, injury, or death occurring at the program, facility, or service while the individual with a disability is under the care of a member of the staff of a program, facility, or service, or by or for a program, facility, or service, that describe any or all of the following: (A) Abuse, neglect, injury, or death. (B) The steps taken to investigate the incidents. (C) Reports and records, including, but not limited to, personnel records prepared or maintained by the facility, program, or service in connection with reports of incidents,		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		subject to the following: (i) If a state statute specifies procedures with respect to personnel records, the protection and advocacy agency shall follow those procedures. (ii) Personnel records shall be protected from disclosure in compliance with the fundamental right of privacy established pursuant to Section 1 of Article I of the California Constitution. The custodian of personnel records shall have a right and a duty to resist attempts to allow the unauthorized disclosure of personnel records, and may not waive the privacy rights that are guaranteed pursuant to Section 1 of Article I of the California Constitution. (D) Supporting information that was relied upon in creating a report, including, but not limited to, all information and records that document interviews with persons who were interviewed, physical and documentary evidence that was reviewed, or related investigative findings. (3) Discharge planning records. (c) Information in the possession of a program, facility, or service that must be available to the agency investigating instances of abuse or neglect pursuant to paragraph (1) of subdivision (a) of Section 4902, whether written or in another medium, draft or final, including, but not limited to, handwritten notes, electronic files, photographs, videotapes, audiotapes, or records, shall include, but not be limited to, all of the following: (1) Information in reports prepared by individuals and entities performing certification or licensure reviews, or by professional accreditation organizations, as well as related assessments prepared for a program, facility, or service by its staff, contractors, or related entities, subject to any other provision of state law protecting records produced by medical care evaluation or peer review committees. (2) Information in professional, performance, building, or other safety standards, or demographic and statistical information, relating to the facility. (d) The authority of the protection and advocacy agency to have access to records does not supersede any prohibition on discovery specified in Sections 1157 and 1157.6 of the Evidence Code, nor does it supersede any prohibition on disclosure subject to the physician-patient privilege or the psychotherapist-patient privilege. (e) (1) The protection and advocacy agency shall have access to records of individuals described in paragraph (1) of subdivision (a) of Section 4902 and in subdivision (a), and other records that are relevant to conducting an investigation, under the circumstances described in those subdivisions, not later than three business days after the agency makes a written request for the records involved. (2) The protection and advocacy agency shall have immediate access to the records, not later than 24 hours after the agency makes a request, without consent from another party, in a situation in which treatment, services, supports, or other assistance is		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		provided to an individual with a disability, if the agency determines there is probable cause to believe that the health or safety of the individual is in serious and immediate jeopardy, or in a case of death of an individual with a disability. (f) Confidential information kept or obtained by the protection and advocacy agency shall remain confidential and may not be subject to disclosure. This subdivision shall not, however, prevent the protection and advocacy agency from doing any of the following: (1) Sharing the information with the individual client who is the subject of the record or report or other document, or with his or her legally authorized representative, subject to any limitation on disclosure to recipients of mental health services as provided in subsection (b) of Section 10806 of Title 42 of the United States Code. (2) Issuing a public report of the results of an investigation that maintains the confidentiality of individual service recipients. (3) Reporting the results of an investigation to responsible investigative or enforcement agencies should an investigation reveal information concerning the facility, its staff, or employees warranting possible sanctions or corrective action. This information may be reported to agencies that are responsible for facility licensing or accreditation, employee discipline, employee licensing or certification suspension or revocation, or criminal prosecution. (4) Pursuing alternative remedies, including the initiation of legal action. (5) Reporting suspected elder or dependent adult abuse pursuant to the Elder Abuse and Dependent Adult Civil Protection Act (Chapter 11 (commencing with Section 15600) of Part 3 of Division 9). (g) The protection and advocacy agency shall inform and train employees as appropriate regarding the confidentiality of client records.		
WIC § 4514. Confidential information and records; disclosure; consent	**Persons with disabilities**	All information and records obtained in the course of providing intake, assessment, and services under Division 4.1 (commencing with Section 4400), Division 4.5 (commencing with Section 4500), Division 6 (commencing with Section 6000), or Division 7 (commencing with Section 7100) to persons with developmental disabilities shall be confidential. Information and records obtained in the course of providing similar services to either voluntary or involuntary recipients prior to 1969 shall also be confidential. Information and records shall be disclosed only in any of the following cases… http://law.onecle.com/california/welfare/4514.html		• Collection, Request, Use, & Disclosure
WIC § 9401. Disclosure of client information	**Older persons** Local public social services agencies providing services to older persons may share	**Area agencies on aging and other county agencies that provide services to older adults through an established multidisciplinary team, including the county departments of public social services, health, mental health, alcohol and drug abuse, and the public guardian, may provide information regarding older adult**		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
	information for coordination of multidisciplinary team activities.	**clients only to other county agencies with staff designated as members of a multidisciplinary team that are, or may be, providing services to the same individuals for purposes of identifying and coordinating the treatment of individuals served by more than one agency**. The county patients' rights advocate shall report any negative consequences of the implementation of this exception to confidentiality requirements to the local mental health director.		
Family Code 7613. Natural father of child conceived by artificial insemination; conditions	**Artificial insemination** Papers and records pertaining to artificial insemination are subject to inspection only upon an order of the court for good cause shown.	If, under the supervision of a licensed physician and surgeon and with the consent of her husband, a wife is inseminated artificially with semen donated by a man not her husband, the husband is treated in law as if he were the natural father of a child thereby conceived. The husband's consent must be in writing and signed by him and his wife. The physician and surgeon shall certify their signatures and the date of the insemination, and retain **the husband's consent as part of the medical record, where it shall be kept confidential and in a sealed file**. However, the physician and surgeon's failure to do so does not affect the father and child relationship. All papers and records pertaining to the insemination, whether part of the permanent record of a court or of a file held by the supervising physician and surgeon or elsewhere, are subject to inspection only upon an order of the court for good cause shown.		• Collection, Request, Use, & Disclosure
Health & Safety § 103850. Confidentiality of information; maintenance of records; research; disclosure; protocols; reports and statistical compilations; violations; personal access	**Birth defects monitoring program** Use, disclosure and access controls for **birth defects monitoring program** and its contractors, researchers	103850. (a) **All information collected pursuant to this chapter shall be confidential and shall be used solely for the purposes provided in this chapter**. For purposes of this chapter, this information shall be referred to as "confidential information." **Access to confidential information shall be limited to authorized program staff, and persons with a valid scientific interest, who meet qualifications as determined by the director, who are engaged in demographic, epidemiological or other similar studies related to health, and who agree, in writing, to maintain confidentiality.** (b) The department shall maintain an accurate record of all persons who are given access to confidential information. The record shall include: the name of the person authorizing access; name, title, address, and organizational affiliation of persons given access; dates of access; and the specific purpose for which information is to be used. The record of access shall be open to public inspection during normal operating hours of the state department. (c) All research proposed to be conducted by persons other than program staff, using confidential information in the system, shall first be reviewed and approved by the director and the State Committee for the Protection of Human Subjects. Satisfaction of the terms of the director's rules for data access shall be deemed to establish a valid scientific interest for purposes of subdivision (a), entitling the researcher to review		• Collection, Request, Use, & Disclosure • Access to Information • Access Controls

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		records collected pursuant to Section 103830 and to contact case subjects and controls. Before confidential information is disclosed pursuant to this section to any other person, agency, or organization, the requesting entity shall demonstrate to the department that the entity has established the procedures and ability to maintain the confidentiality of the information. (d) Notwithstanding any other provision of law, any disclosure authorized by this section shall include only the information necessary for the stated purpose of the requested disclosure, and shall be made only upon written agreement that the information will be kept confidential, used for the approved purpose, and not be further disclosed. (e) The furnishing of confidential information to the department or its authorized representative in accordance with this section shall not expose any person, agency, or entity furnishing the information to liability, and shall not be considered a waiver of any privilege or a violation of a confidential relationship. (f) Whenever program staff, pursuing program objectives, deems it necessary to contact case subjects and controls, program staff shall submit a protocol describing the research to the director and to the State Committee for the Protection of Human Subjects. Once a protocol is approved by that committee, program staff shall be deemed to have established a bona fide research purpose, and shall be entitled to complete the approved project and contact case subjects and controls without securing any additional approvals or waivers from any entity. (g) Notwithstanding any other provision of law, no part of the confidential information shall be available for subpoena, nor shall it be disclosed, discoverable, or compelled to be produced in any civil, criminal, administrative, or other proceeding, nor shall this information be deemed admissible as evidence in any civil, criminal, administrative, or other tribunal or court for any reason. Nothing in this section shall prohibit the publishing by the department of reports and statistical compilations relating to birth defects, stillbirth, or miscarriage that do not in any way identify individual cases or individual sources of information. (h) Any person who, in violation of a written agreement to maintain confidentiality, discloses any information provided pursuant to this section, or who uses information provided pursuant to this section in a manner other than as approved pursuant to this section may be denied further access to any confidential information maintained by the department. That person shall also be subject to a civil penalty of five hundred dollars ($500). The penalty provided in this section shall not be construed as restricting any remedy, provisional or otherwise, provided by law for the benefit of the department or any person. (i) Notwithstanding the restrictions in this section, an individual to whom the information pertains shall have access to his or her own information in accordance with Chapter 1 (commencing with Section 1798) of Title 1.8 of the Civil Code.		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
Disclosure of Genetic Test Results by a Health Care Service Plan, Cal. Civ. Code § 56.17	**Genetic testing** Disclosures of genetic testing lab results	(a) This section shall apply to the **disclosure of genetic test results contained in an applicant's or enrollee's medical records by a health care service plan**. (b) **Any person who negligently discloses results of a test for a genetic characteristic to any third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply, except pursuant to a written authorization as described in subdivision (g), shall be assessed a civil penalty** in an amount not to exceed one thousand dollars ($1,000) plus court costs, as determined by the court, which penalty and costs shall be paid to the subject of the test. (c) Any person who willfully discloses the results of a test for a genetic characteristic to any third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply, except pursuant to a written authorization as described in subdivision (g), shall be assessed a civil penalty in an amount not less than one thousand dollars ($1,000) and no more than five thousand dollars ($5,000) plus court costs, as determined by the court, which penalty and costs shall be paid to the subject of the test. (d) Any person who willfully or negligently discloses the results of a test for a genetic characteristic to a third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply, except pursuant to a written authorization as described in subdivision (g), that results in economic, bodily, or emotional harm to the subject of the test, is guilty of a misdemeanor punishable by a fine not to exceed ten thousand dollars ($10,000). (e) In addition to the penalties listed in subdivisions (b) and (c), any person who commits any act described in subdivision (b) or (c) shall be liable to the subject for all actual damages, including damages for economic, bodily, or emotional harm which is proximately caused by the act. (f) Each disclosure made in violation of this section is a separate and actionable offense. (g) The applicant's "written authorization," as used in this section, shall satisfy the following requirements: (1) Is written in plain language and is in a typeface no smaller than 14-point type. (2) Is dated and signed by the individual or a person authorized to act on behalf of the individual. (3) Specifies the types of persons authorized to disclose information about the individual. (4) Specifies the nature of the information authorized to be disclosed. (5) States the name or functions of the persons or entities authorized to receive the information.		• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		(6) Specifies the purposes for which the information is collected. (7) Specifies the length of time the authorization shall remain valid. (8) Advises the person signing the authorization of the right to receive a copy of the authorization. Written authorization is required for each separate disclosure of the test results. (h) This section shall not apply to disclosures required by the Department of Health Services necessary to monitor compliance with Chapter 1 (commencing with Section 124975) of Part 5 of Division 106 of the Health and Safety Code, nor to disclosures required by the Department of Managed Care necessary to administer and enforce compliance with Section 1374.7 of the Health and Safety Code. (i) For purposes of this section, "genetic characteristic" has the same meaning as that set forth in subdivision (d) of Section 1374.7 of the Health and Safety Code.		
California Civil Code Section 56.17 (2003)	**Genetic testing** Genetic test results in application or medical records of a health plan	56.17. (a) This section shall apply to the disclosure of **genetic test results contained in an applicant's or enrollee's medical records by a health care service plan**. (b) Any person who negligently discloses results of a test for a genetic characteristic to any third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply, except pursuant to a written authorization as described in subdivision (g), shall be assessed a civil penalty in an amount not to exceed one thousand dollars ($1,000) plus court costs, as determined by the court, which penalty and costs shall be paid to the subject of the test. (c) Any person who willfully discloses the results of a test for a genetic characteristic to any third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply, except pursuant to a written authorization as described in subdivision (g), shall be assessed a civil penalty in an amount not less than one thousand dollars ($1,000) and no more than five thousand dollars ($5,000) plus court costs, as determined by the court, which penalty and costs shall be paid to the subject of the test. (d) Any person who willfully or negligently discloses the results of a test for a genetic characteristic to a third party in a manner that identifies or provides identifying characteristics of the person to whom the test results apply, except pursuant to a written authorization as described in subdivision (g), that results in economic, bodily, or emotional harm to the subject of the test, is guilty of a misdemeanor punishable by a fine not to exceed ten thousand dollars ($10,000). (e) In addition to the penalties listed in subdivisions (b) and (c), any person who commits any act described in subdivision (b) or (c) shall be liable to the subject for all actual damages, including damages for economic, bodily, or emotional harm which is proximately caused by the act. (f) Each disclosure made in violation of this section is a separate and actionable	Prohibits a health care service plan from disclosing your genetic test results without specific written permission.	• Collection, Request, Use, & Disclosure

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		offense. (g) The applicant's "written authorization," as used in this section, shall satisfy the following requirements: (1) Is written in plain language and is in a typeface no smaller than 14-point type. (2) Is dated and signed by the individual or a person authorized to act on behalf of the individual. (3) Specifies the types of persons authorized to disclose information about the individual. (4) Specifies the nature of the information authorized to be disclosed. (5) States the name or functions of the persons or entities authorized to receive the information. (6) Specifies the purposes for which the information is collected. (7) Specifies the length of time the authorization shall remain valid. (8) Advises the person signing the authorization of the right to receive a copy of the authorization. Written authorization is required for each separate disclosure of the test results. (h) This section shall not apply to disclosures required by the Department of Health Services necessary to monitor compliance with Chapter 1 (commencing with Section 124975) of Part 5 of Division 106 of the Health and Safety Code, nor to disclosures required by the Department of Managed Care necessary to administer and enforce compliance with Section 1374.7 of the Health and Safety Code. (i) For purposes of this section, "genetic characteristic" has the same meaning as that set forth in subdivision (d) of Section 1374.7 of the Health and Safety Code.		
Health & Safety § 124980. Regulations and standards; principles; damages for breach of confidentiality	**Hereditary diseases/congenital defects** Use, disclosure, and consent to disclose information related to hereditary diseases/congenital defects	124980. The director shall establish any regulations and standards for hereditary disorders programs as the director deems necessary to promote and protect the public health and safety. Standards shall include licensure of master level genetic counselors and doctoral level geneticists. Regulations adopted shall implement the principles established in this section. These principles shall include, but not be limited to, the following: (a) The public, especially communities and groups particularly affected by programs on hereditary disorders, should be consulted before any regulations and standards are adopted by the department. (b) The incidence, severity, and treatment costs of each hereditary disorder and its perceived burden by the affected community should be considered and, where appropriate, state and national experts in the medical, psychological, ethical, social, and economic effects or programs for the detection and management of hereditary disorders shall be consulted by the department.		• Collection, Request, Use, & Disclosure • Consent

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		(c) Information on the operation of all programs on hereditary disorders within the state, except for confidential information obtained from participants in the programs, shall be open and freely available to the public. (d) Clinical testing procedures established for use in programs, facilities, and projects shall be accurate, provide maximum information, and the testing procedures selected shall produce results that are subject to minimum misinterpretation. (e) No test or tests may be performed on any minor over the objection of the minor's parents or guardian, nor may any tests be performed unless the parent or guardian is fully informed of the purposes of testing for hereditary disorders and is given reasonable opportunity to object to the testing. (f) No testing, except initial screening for phenylketonuria (PKU) and other diseases that may be added to the newborn screening program, shall require mandatory participation, and no testing programs shall require restriction of childbearing, and participation in a testing program shall not be a prerequisite to eligibility for, or receipt of, any other service or assistance from, or to participate in, any other program, except where necessary to determine eligibility for further programs of diagnoses of or therapy for hereditary conditions. (g) Pretest and posttest counseling services for hereditary disorders shall be available through the program or a referral source for all persons determined to be or who believe themselves to be at risk for a hereditary disorder. Genetic counseling shall be provided by a physician, a certified advanced practice nurse with a genetics specialty, or other appropriately trained licensed health care professional and shall be nondirective, shall emphasize informing the client, and shall not require restriction of childbearing. (h) All participants in programs on hereditary disorders shall be protected from undue physical and mental harm, and except for initial screening for phenylketonuria (PKU) and other diseases that may be added to newborn screening programs, shall be informed of the nature of risks involved in participation in the programs, and those determined to be affected with genetic disease shall be informed of the nature, and where possible the cost, of available therapies or maintenance programs, and shall be informed of the possible benefits and risks associated with these therapies and programs. (i) All testing results and personal information generated from hereditary disorders programs shall be made available to an individual over 18 years of age, or to the individual's parent or guardian. If the individual is a minor or incompetent, all testing results that have positively determined the individual to either have, or be a carrier of, a hereditary disorder shall be given through a physician or other source of health care. (j) All testing results and personal information from hereditary disorders programs obtained from any individual, or from specimens from any individual, shall be held confidential and be considered a confidential medical record except for information that		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		the individual, parent, or guardian consents to be released, provided that the individual is first fully informed of the scope of the information requested to be released, of all of the risks, benefits, and purposes for the release, and of the identity of those to whom the information will be released or made available, except for data compiled without reference to the identity of any individual, and except for research purposes, provided that pursuant to Subpart A (commencing with Section 46.101) of Part 46 of Title 45 of the Code of Federal Regulations entitled "Basic HHS Policy for Protection of Human Subjects," the research has first been reviewed and approved by an institutional review board that certifies the approval to the custodian of the information and further certifies that in its judgment the information is of such potentially substantial public health value that modification of the requirement for legally effective prior informed consent of the individual is ethically justifiable. (k) A physician providing information to patients on expanded newborn screening shall disclose to the parent the physician's financial interest, if any, in the laboratory to which the patient is being referred. (l) An individual whose confidentiality has been breached as a result of any violation of the provisions of the Hereditary Disorders Act, as defined in subdivision (b) of Section 27, may recover compensatory and civil damages. Any person who negligently breaches the confidentiality of an individual tested under this article shall be subject to civil damages of not more than ten thousand dollars ($10,000), reasonable attorney's fees, and the costs of litigation. Any person who knowingly breaches the confidentiality of an individual tested under this article shall be subject to payment of compensatory damages, and in addition, may be subject to civil damages of fifty thousand dollars ($50,000), reasonable attorney's fees, and the costs of litigation, or imprisonment in the county jail of not more than one year. If the offense is committed under false pretenses, the person may be subject to a fine of not more than one hundred thousand dollars ($100,000), imprisonment in the county jail of not more than one year, or both. If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, the person may be subject to a fine of not more than two hundred fifty thousand dollars ($250,000), imprisonment in the county jail of not more than one year, or both. (m) "Genetic counseling" as used in this section shall not include communications that occur between patients and appropriately trained and competent licensed health care professionals, such as physicians, registered nurses, and physician's assistants who are operating within the scope of their license and qualifications as defined by their licensing authority.		
Use and Disclosure of Medical Information by Employers, Cal. Civ. Code §§ 56.20-56.25.	**Employer obtained medical information**	(a**) Each employer who receives medical information shall establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information. These procedures may include, but are not**		

Citation	Applicability	Content of Law	Notes/ Associated Citations	Associated Guideline
		limited to, instruction regarding confidentiality of employees and agents handling files containing medical information, and security systems restricting access to files containing medical information		

Appendix J: Other States' Consent Model

State	Method of Opt-In	Laws/Policies/ Acts/etc.	Language	Consent Form	Education
Arizona	Pending?	Arizona Senate Bill 1258	SB 1258		
California	Policy	CalPSAB			
Colorado	State designated entity CORHIO (Co Regional Health Information Organization) facilitates HIE		State HIE Strategic Plan	CORHIO Opt In Form	
Florida	Policy In Development	Florida Health Information Network	Health Information Exchange Legal Work Group Draft 8-6-10 (bottom of pg 2, top of pg 3)		
Massachusetts	State Law (Massachusetts Strategic Plan references Chapter 305 of MA law)	Chapter 305 of MA State Law	Chapter 305: "Section 6F"		

State	Method of Opt-In	Laws/Policies/ Acts/etc.	Language	Consent Form	Education
Minnesota	State Law (Minnesota Health Records Act of 2007)		Health Records Act: "Subd. 4. Notice of rights; information on release" (Line 349.1)	Minnesota Standard Consent Form to Release Health Information	
New Mexico	Patient consent is always required before patient information can be accessed through NMHIC	New Mexico Electronic Medical Records Act	New Mexico Electronic Medical Records Act (Page 98 of Document) NMHIE Strategic and Operational Plans - S.13.1 Privacy And Security (Page 48 of Document)		
New York	State Law requires written consent for the disclosure of mental health information and provides no exceptions to this requirement.			Health Information Exchange NY (HIXNY) Consent Form Long Island RHIO Consent Form Rochester RHIO Consent Form HIPAA Consent Form	

State	Method of Opt-In	Laws/Policies/ Acts/etc.	Language	Consent Form	Education
Nevada	Law in Development	SB 43 Sec. 15. NRS 439.538	Senate Committee Minutes (2-17-11)		"We are an 'Opt In' State" 7-12-11 Blog post
North Carolina	Policy	Opt-in or mixed with partial Opt-out	Legal/Policy Workgroup, NC HIE Board (Word doc file)		
Ohio	Policy	Policy put forth by Ohio Health Information Partnership Privacy and Policy Committee	"Research and Recommendation for Patient Consent Policies for Ohio's Statewide Health Information Exchange"		Patient Privacy Law Fact Sheet
Oklahoma	Senate Bill	Senate Bill 1420 of 2008 "Oklahoma Health Information Act"	State Legislature ordered the creation of a standard authorization form for health information exchange. Providers who use the optional form and follow are immunized from liability under state privacy laws (from pdf doc, info on page 4)	http://okhca.org/provider/forms/pdflib/hca-20.pdf	

State	Method of Opt-In	Laws/Policies/ Acts/etc.	Language	Consent Form	Education
Rhode Island	Policy, State Law (?)		Rhode Island Statute (CHAPTER 5-37.3):		
Vermont	Policy	Mental health care provisions, 18 VSA § 7103(a)	Vermont Statute 18 V.S.A. § 7103		
Washington	Policy	Four Health Record Bank pilot programs			

Appendix K: Patient Informing Material

Details About the Electronic Exchange of Individual Health Information and the Consent Process

CONSENT

How Your Information Will be Used. Your electronic individual health information will be used by [Name of Provider Organization/HIE] Health Information Exchange (HIE) **only** to:
• Provide you with medical treatment and related services
• Evaluate and improve the quality of medical care provided to you and all patients

The decision to participate in the [Name of HIE] HIE is voluntary. No health care provider participating in the HIE will deny you medical care and your insurance eligibility will not be affected by your choice to participate or not participate.

The benefits of the electronic exchange of individual health information are:

- Improved quality of care based on more complete information regarding your past condition(s) and treatment,
- Improved coordination of care between all of your health care providers,
- Decrease in the duplication of care or provision of unnecessary care, and
- Decrease of delays in treatment.

Some potential risks associated with the electronic exchange of individual health information include:

- Unauthorized disclosure of your individual health information, and
- Identity theft if there is a breach of your health care provider's electronic files.

PURPOSE

The purpose of giving permission to electronically exchange your individual health information is to allow all aspects of your medical history to be taken into account when determining your current and future care. As a result of increased access to information, your providers can make well-informed decisions in your medical care which should result in improved care at hospitals, physician offices, labs, pharmacies,

etc. Additionally, allowing your electronic health information to be exchanged should help with the protection of the public as a whole such as in the event of an epidemic (for example the H1N1 virus) or other public health crises.

TYPES OF INFORMATION INCLUDED IN THIS CONSENT

What Types of Information about You Are Included? If you give consent, [Name of Provider Organization] may access ALL of your electronic health information available through the [Name of HIE] HIE. This includes information created before and after the date of your Consent Form. Your health records may include a history of illnesses or injuries you have had (like diabetes or a broken bone), test results (like X-rays or blood tests), and lists of medicines you have taken. This information may relate to sensitive health conditions, including but not limited to:

- Alcohol or illicit drug use
- Contraception and abortion (family planning)
- Genetic (inherited) conditions or tests for these
- HIV/AIDS
- Mental health conditions
- Sexually transmitted diseases

Where Health Information About You Comes From. Information about your health comes from places that have provided you with health care. These may include hospitals, physicians' offices, pharmacies, clinical laboratories, Medi-Cal, and other organizations that exchange health information electronically. A complete list of current Information Sources is available from [Name of Provider Organization, or HIE, as applicable]. The list of participating organizations may change in the future.

Who May Access Information About You, If You Give Consent? Individuals legally allowed to access your electronic individual health information would be allowed to view your records. An example of those who may access information about you: doctors and other health care providers who serve on [Name of Provider Organization]'s medical staff and who are involved in your medical care; health care providers who are covering or on call for [Name of Provider Organization]'s doctors; hospitals, clinics, pharmacies, labs, other licensed providers, health information organizations (HIOs), and health care staff members who carry out activities permitted by this Consent Form as described in the Consent paragraph above.

Penalties for Improper Access to or Use of Your Information. There is some risk associated with the electronic exchange of individual health information.

There are penalties for inappropriate access to or use of your electronic health information for non-clinical reasons/purpose. If at any time you suspect that someone has accessed your electronic individual health information inappropriately, call [Name of Provider Organization] at: [Phone Number of Provider Organization]; or visit [Name of Provider Organization]'s website, Office of Civil Rights' website www.hhs.gov/ocr/, California Department of Public Health's website www.cdph.ca.gov, or the California Office of Health Information Integrity's (CalOHII) website www.calohi.ca.gov. You can also reference California Civil Code Sections 56.35 and 56.36.

Re-disclosure of Information. Electronic health information about you may be re-disclosed by [Name of Provider Organization] to others only to the extent permitted by state and federal laws and regulations. This is also true of health information about you that exists in a paper form. Some state and federal laws provide special protections for certain kinds of sensitive health information, including HIV/AIDS, drug and alcohol treatment, contraception and abortion (family planning), genetic (inherited) conditions or tests, mental health conditions, and sexually transmitted diseases. These special requirements must be followed whenever people receive these kinds of sensitive health information. [Name of Provider Organization/HIE] and persons who access this information through the [Name of HIE] must comply with these requirements.

Withdrawing Your Consent. You can withdraw your consent at any time by signing a Withdrawal of Consent Form and giving it to [Name of Provider Organization]. You can also change your consent choices by signing a new Consent Form at any time. You can get these forms from [Name of Provider Organization]. In the event that you withdraw your consent, your individual health information will continue to be stored electronically, but will not be accessible through [Name of the HIE].

Effective Period. Your Consent Form will remain in effect until you withdraw your consent.

Note: Providers who access your electronic individual health information through [Name of HIE] while your consent is in effect may copy or include your information in their own electronic health records system. Even if you later decide to withdraw your consent, they are not required to remove it from their records.

Copy of Form. You are entitled to get a copy of your Consent Form after you sign it.

Appendix L: Patient Consent Form

Patient Consent Form for Electronic Exchange of Individual Health Information	For Provider Use: MRN_____

PLEASE READ THIS ENTIRE DOCUMENT BEFORE SIGNING THE CONSENT FORM.

Please provide the following information:

_____

PATIENT NAME Last First Middle

PREVIOUS NAME(S) _____ **GENDER:** M__F___

_____

STREET ADDRESS/P. O BOX

CITY _____ **STATE** _____ **ZIP CODE** _____

PHONE NUMBER (OPTIONAL) _____

DATE OF BIRTH (MM)_____(DD)_____(YYYY)_____

CONSENT: I understand that if I give consent below, I am allowing [Name of Provider Organization] to release and/or access ALL of my electronically available individual health information. Electronically available individual health information may include information from my health care providers, including hospitals, physicians, clinics, pharmacies, labs, and other licensed providers, as well as a third party organization (called a Health Information Organization (HIO)) that assists in the exchange of my information.

PURPOSE: I understand that my individual health information that is electronically disclosed to health care providers may be used to provide me with medical treatment, assess/improve the quality of my medical care, and to facilitate public health reporting. Examples of health care providers include, but are not limited to, the following: physicians, nurses, hospitals, clinics, pharmacies, labs, other licensed providers, heath care staff, and HIOs.

TYPES OF INFORMATION INCLUDED IN THIS CONSENT: I understand that this consent permits [Name of Provider Organization] to access and disclose ALL of my electronically available individual health information, including but not limited to, information related to drug/alcohol

abuse, HIV/AIDS testing, status or treatment; genetic diseases or genetic tests; family planning/reproductive care; sexually transmitted diseases; mental health, emergency care records, nursing notes, laboratory results, pathology reports, x-ray reports, films, and all other individual health information as allowable under applicable law.

YOUR SIGNATURE: I understand that my consent becomes effective upon signing this form and will remain in effect until I submit a written request to revoke it. I understand that I have the right to withdraw or revoke this consent in writing at any time, except to the extent that the electronic health information has already been released to another entity. This consent permits access to and disclosure of my individual health information created both before and after the date I sign this form.

My Consent Choices:

☐ ***I GIVE CONSENT FOR [Name of Provider Organization] to release and/or access ALL of my electronic health information through health information organization(s) in connection with providing me any health care services, including emergency care.***

☐ ***I DENY CONSENT FOR [Name of Provider Organization] to release and/or access any of my electronic health information through health information organization(s) EXCEPT in the event of a medical emergency.***

☐ ***I DENY CONSENT FOR [Name of Provider Organization] to release and/or access any of my electronic health information through health information organization(s) even in the event of a medical emergency.***

Signature of patient or authorized representative:
If I sign this form as the Patient's Authorized Representative, I understand that all references in this form to "I", "me" or "my" refer to the Patient.

_____ _____
Date

If signed by someone other than the patient, print name and indicate relationship:

_____ _____ _____
Authorized Representative *Relationship* *Date*

Address of authorized representative signing this form (please print):

_____

Phone number of authorized representative signing this form:

_____

Signature of witness:

Witness required only for telephone consent, physical inability to sign, or signature by mark. Telephone consent is subject to verification of identity.

_____ _____ _____

Witness *Relationship* *Date*

Appendix M: Assembly Bill 278: Health Information Exchange: Demonstration Projects

BILL NUMBER: AB 278 CHAPTERED
BILL TEXT

CHAPTER 227
FILED WITH SECRETARY OF STATE SEPTEMBER 24, 2010
APPROVED BY GOVERNOR SEPTEMBER 23, 2010
PASSED THE SENATE AUGUST 19, 2010
PASSED THE ASSEMBLY AUGUST 26, 2010
AMENDED IN SENATE AUGUST 17, 2010
AMENDED IN SENATE JULY 15, 2010
AMENDED IN SENATE JUNE 21, 2010
AMENDED IN SENATE JUNE 3, 2010

INTRODUCED BY Assembly Member Monning

FEBRUARY 12, 2009

An act to add and repeal Division 109.6 (commencing with Section 130275) of the Health and Safety Code, relating to health information.

LEGISLATIVE COUNSEL'S DIGEST

AB 278, Monning. Health information exchange: demonstration projects.

Existing law establishes the Office of Health Information Integrity within the California Health and Human Services Agency to ensure the enforcement of state law mandating confidentiality of medical information and to impose administrative fines for the unauthorized use of medical information. Existing law authorizes the California Health and Human Services Agency, or one of the departments under its jurisdiction, to apply for federal funds made available through the federal American Recovery and Reinvestment Act of 2009 (ARRA) for health information technology and exchange.

This bill would authorize the office to establish and administer demonstration projects to evaluate potential solutions to facilitate health information exchange that promote quality of care, respect the privacy and security of personal health information, and enhance the trust of the stakeholders. This bill would authorize health care entities or governmental authorities, as defined, that receive,

share, exchange, or use a California resident's medical information to submit an application with the office to be approved as demonstration project participants, as defined. The bill would authorize the office to approve annually up to 4 projects as demonstration projects. The bill would require any costs associated with the support, assistance, and evaluation of approved demonstration projects to be funded exclusively by the above-described federal funds or other non-General Fund sources. The bill would require the office to report to prescribed committees of the Legislature within 6 months after the end of the project.

This bill would become inoperative on the date the Director of the Office of Health Information Integrity executes a declaration stating that the grant period for the above-described federal funds has ended, and as of that date would be repealed.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Division 109.6 (commencing with Section 130275) is added to the Health and Safety Code, to read:

DIVISION 109.6. Health Information Exchange Privacy and Security Demonstration Projects

130275. The Legislature finds and declares all of the following:

(a) There is a need to enhance California's ability to obtain and use federal funding, as awarded in the State Cooperative Grant Agreement for health information exchange, for the establishment of statewide health information exchange infrastructure in California. The California Health and Human Services Agency is authorized by the Legislature, under Section 130255, to use those federal funds to achieve that purpose.

(b) Health information exchange has the potential to significantly improve the quality of treatment and care, reduce unnecessary health care costs, and increase administrative efficiencies within the health care system. The application of health information exchange technology to manage health information will also have a significant impact on consumers, health care facilities, and licensed health care providers.

(c) Current laws may not adequately protect privacy, or may impose obstacles to the exchange of vital health information, as required by the State Cooperative Grant Agreement for health information exchange and other federal health information funding programs.

(d) It is the intent of the Legislature to authorize the Office of Health Information Integrity within the California Health and Human Services Agency to establish and administer demonstration projects funded by federal grants and other sources. It is the intent of the Legislature that the demonstration projects do all of the following:

(1) Identify barriers to implementing health information exchanges.

(2) Test potential security and privacy policies for the safe and secure exchange of health information, including, but not limited to, issues related to access to, and storage of, individual health information.

(3) Identify and address differences between state and federal laws regarding privacy of health information.

130276. For purposes of this division, the following definitions apply:

(a) "Demonstration project" means a project approved and administered by the office in accordance with this division and the State Cooperative Grant Agreement for health information exchange or any other similar grant or grants.

(b) "Demonstration project participant" means a health care entity that is approved by the office to participate in a demonstration project.

(c) "Director" means the Director of the Office of Health Information Integrity.

(d) "Governmental authority" means any municipal, county, state, or other governmental entity that has jurisdiction and control over the provision of, or payment for, medical services or that routinely receives medical information to complete its designated governmental function.

(e) "Health information exchange service participant" means a health care entity that has voluntarily agreed to use the health information exchange services developed in accordance with this division.

(f) "Meaningful use" means the term as defined in the federal Health Information Technology for Economic and Clinical Health Act (HITECH Act) (Public Law 111-5) and the regulations promulgated thereunder.

(g) "Office" means the Office of Health Information Integrity.

(h) "State Cooperative Grant Agreement" means the grant agreement between the federal government and the state in which the federal government awarded the state with grant money pursuant to the HITECH Act in February 2010.

130277. The director may adopt regulations to ensure all approved health information exchange service participants and demonstration project participants follow rules, and work within parameters, as defined by the office, that are consistent for the exchange of information.

130278. Before adopting regulations pursuant to Section 130277, the office shall adopt the following standards:

(a) At least 45 days prior to adoption, the office shall post a proposed regulation on its Internet Web site. Public comment shall be accepted by the office for at least 30 days after the proposed regulation is posted. If a member of the public requests a public hearing during the 30-day review period, the hearing shall be held prior to adoption of the regulation. The process described in this subdivision shall apply to the adoption of new regulations and to changes to existing regulations.

(b) Adoption of, and changes to, regulations adopted pursuant to

this division shall not be subject to the rulemaking requirements of Section 11343.4 and Article 5 (commencing with Section 11346) and Article 6 (commencing with Section 11349) of Chapter 3.5 of Part 1 of Division 3 of Title 2 of the Government Code.

(c) The director shall file any regulation adopted pursuant to Section 130277 with the Office of Administrative Law for filing with the Secretary of State and publication in the California Code of Regulations. Any regulation filed with the Office of Administrative Law pursuant to this subdivision shall include a citation to this section and any other applicable state or federal laws as providing authority for the adoption of the regulation.

(1) Any regulation adopted pursuant to Section 130277 shall become effective on the date it is filed with the Secretary of State unless the director prescribes a later date in the regulation or in a written instrument filed with the regulation.

(2) Any regulation adopted pursuant to Section 130277 shall expire the date that this division is repealed.

130279. (a) The California Health and Human Services Agency, through the office, may establish and administer demonstration projects to evaluate potential solutions to facilitate health information exchange that promote quality of care, respect the privacy and security of personal health information, and enhance the trust of the stakeholders.

(b) Health care entities or governmental authorities, that receive, share, exchange, or use a California resident's medical information, may submit an application with the office to be approved as demonstration project participants. Upon receiving an application, the office shall do both of the following:

(1) Assist applicants in soliciting federal funds for the demonstration projects.

(2) Work with applicants to define the scope of the demonstration project.

(c) The director may approve demonstration projects to test for, but not limited to, any of the following areas:

(1) Policies and practices related to patient consent, informing, and notification.

(2) New technologies and applications that enable the transmission of protected health information, while increasing privacy protections by ensuring only required health data is transmitted for purposes and uses consistent with state and federal law.

(3) Implementation issues, if any, encountered by small solo health care providers as a result of exchanging electronic health information.

(d) The selection of demonstration projects shall be based on, but not limited to, the following criteria:

(1) Areas critical to building consumer trust and confidence in the health information exchange system.

(2) Projects that help support the exchange of information critical to meeting the federal meaningful use provisions.

(3) Areas recommended by the California health information exchange consumer and industry stakeholder advisory process.

(e) The office shall engage with health care stakeholders to evaluate issues identified by the demonstration projects, comment upon proposed regulations, and discuss solutions for health information exchange.

(f) The office may annually approve up to four projects, as demonstration projects.

(g) The office shall work collaboratively with approved demonstration project participants to identify a set of common data elements that will be used to collect, analyze, and measure performance.

(h) The office shall receive reports from the demonstration project participants on the outcome of the demonstration projects no later than 60 business days after the end of the demonstration project.

130280. (a) The office shall review the results of a demonstration project and, notwithstanding Sections 9795 and 10231.5 of the Government Code, shall report those results to the Joint Legislative Budget Committee, the Senate Committee on Appropriations, the Senate Committee on Budget and Fiscal Review, the Senate Committee on Health, the Assembly Committee on Appropriations, the Assembly Committee on Budget, and the Assembly Committee on Health within six months after the end of a demonstration project.

(b) The demonstration projects carried out utilizing federal grant funds may be subject to federal auditing provisions.

130281. Any costs associated with the support, assistance, and evaluation of approved demonstration projects shall be funded exclusively by federal funds or other non-General Fund sources.

130282. This division shall become inoperative on the date the director executes a declaration stating that the grant period for the State Cooperative Grant Agreement for health information exchange has ended, and as of that date is repealed.